

## DATA PROCESSING ADDENDUM

Last Modified: January 16, 2023

This Data Processing Addendum, including its Schedules, (“DPA”) forms part of the Software and Support Agreement or other written or electronic agreement between Recognize Services, Inc. (“Recognize”) and Customer for the purchase of SaaS services from Recognize (identified either as “Services” or otherwise in the applicable agreement, and hereinafter defined as “Services”) (the “Agreement”) to reflect the Parties’ agreement with regard to the Processing of Personal Data.

In the course of providing the Services to Customer pursuant to the Agreement, Recognize may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data.

This DPA has been pre-signed on behalf of Recognize Services, Inc.

To enter into this DPA, Customer must:

- (a) have a valid Agreement in place for the provision of Services;
- (b) complete the signature block below by signing and providing all relevant information; and
- (c) submit the completed and signed DPA to Recognize.

Where Customer makes any deletions or other revisions to this DPA, this DPA will be null and void. Customer signatory represents to Recognize that he or she has the legal authority to bind Customer and is lawfully able to enter into this DPA.

### 1. DEFINITIONS

“Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“Authorized Affiliate” means any of Customer’s Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Recognize, but has not signed its own Order Form with Recognize.

“CCPA” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act, and its implementing regulations.

“Controller” means the entity which determines the purposes and means of the Processing of Personal Data.

“Customer” means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Order Forms. For the purposes of this DPA only,

and except where indicated otherwise, the term “Customer” shall include Customer and its Authorized Affiliates.

“Customer Data” means what is defined in the Agreement as “Customer Data”, provided that such data is electronic data and information submitted by or for Customer to the Services.

“Data Protection Laws and Regulations” means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including those of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, Canada, Australia, and the United States and its states.

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

“Europe” means the European Union, the European Economic Area, Switzerland and the United Kingdom.

“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, and repealing Directive 95/46/EC (General Data Protection Regulation), including as implemented or adopted under the laws of the United Kingdom.

“Personal Data” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as Personal Data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

“Processing” or “Process” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means the entity which Processes Personal Data on behalf of the Controller, including as applicable any “service provider” as that term is defined by the CCPA.

“Public Authority” means a government agency or law enforcement authority, including judicial authorities.

“Security and Privacy Documentation” means the Security and Privacy Documentation applicable to the specific Services purchased by Customer, as updated from time to time, and accessible via <https://trust.recognizeapp.com>, or as otherwise made reasonably available by Recognize.

“Standard Contractual Clauses” means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at [https://eurlex.europa.eu/eli/dec\\_impl/2021/914/oj](https://eurlex.europa.eu/eli/dec_impl/2021/914/oj).

“Sub-processor” means any Processor engaged by Recognize.

## **2. DATA PROCESSING**

2.1. Customer's Processing of Personal Data. Customer as Controller or Processor shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of Recognize as Processor (including where the Customer is a Processor, by ensuring that the ultimate Controller does so). For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges and agrees that its use of the Services will not violate the rights of any Data Subject, including those that have opted-out from sales or other disclosures of Personal Data, to the extent applicable under Data Protection Laws and Regulations.

2.2. Recognize's Processing of Personal Data. Recognize shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.3. Details of the Processing. The subject-matter of Processing of Personal Data by Recognize is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Description of Processing/Transfer) to this DPA.

2.4. Customer Instructions. Recognize shall inform Customer immediately (i) if, in its opinion, an instruction from Customer constitutes a breach of the GDPR and/or (ii) if Recognize is unable to follow Customer's instructions for the Processing of Personal Data.

## **3. RIGHTS OF DATA SUBJECTS**

3.1. Data Subject Request. Recognize shall, to the extent legally permitted, promptly notify Customer of any complaint, dispute or request it has received from a Data Subject such as a Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request". Recognize shall not respond to a Data Subject Request itself, except that Customer authorizes Recognize to redirect the Data Subject Request as necessary to allow Customer to respond directly.

3.2. Required Assistance. Taking into account the nature of the Processing, Recognize shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

3.3. Additional Assistance. To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Recognize shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Recognize is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Recognize's provision of such assistance.

#### **4. CONFIDENTIALITY**

Recognize shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Recognize shall (i) ensure that such confidentiality obligations survive the termination of the personnel engagement; (ii) take commercially reasonable steps to ensure the reliability of any Recognize personnel engaged in the Processing of Personal Data; and (iii) ensure that Recognize's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement, any applicable Order Form(s) and Documentation.

#### **5. SUB-PROCESSORS**

5.1. Appointment of Sub-processors. Customer acknowledges and agrees that (a) Recognize's Affiliates may be retained as Sub-processors; and (b) Recognize and Recognize's Affiliates respectively may engage third-party Sub-processors to provide the Services.

Recognize or an Recognize Affiliate has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2. Current List of Sub-processors and Notification of New Sub-processors. The current list of Sub-processors engaged in Processing Personal Data for the performance of each applicable Service, including a description of their processing activities and countries of location, is listed at <https://recognizeapp.com/gdpr/recognize-subprocessors.pdf>

Customer hereby consents to these Sub-processors, their locations and processing activities as it pertains to their Personal Data. Customer shall subscribe to notifications of new Sub-processors for each applicable Service via <https://status.recognizeapp.com>, and if Customer subscribes,

Recognize shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data to provide the applicable Services.

5.3. **Objection Right for New Sub-processors.** Customer may object to Recognize's use of a new Sub-processor by notifying Recognize promptly in writing within thirty (30) days of receipt of Recognize's notice in accordance with the mechanism set out in section

5.2. If Customer objects to a new Sub-processor as permitted in the preceding sentence, Recognize 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 without unreasonably burdening Customer. If Recognize is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Recognize without the use of the objected-to new Sub-processor by providing written notice to Recognize. Recognize will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

5.4. **Liability.** Recognize shall be liable for the acts and omissions of its Sub-processors to the same extent Recognize would be liable if performing the services of each Sub-processor directly under the terms of this DPA, unless otherwise set forth in the Agreement.

## **6. SECURITY, CERTIFICATIONS AND AUDIT**

6.1. **Controls for the Protection of Customer Data.** Recognize shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in the Security and Privacy Documentation. Recognize regularly monitors compliance with these measures. Recognize will not materially decrease the overall security of the Services during a subscription term.

6.2. **Third-Party Certifications and Audits.** Recognize has obtained the third-party certifications and audits set forth in the Security and Privacy Documentation for each applicable Service. Where Recognize has obtained ISO 27001 certifications for a particular Service as described in the Documentation. Recognize agrees to maintain these certifications or standards, or appropriate and comparable successors thereof, for the duration of the Agreement.

6.3. **Audit Program.** Recognize shall make available to Customer information to demonstrate compliance with the obligations set out in this DPA, including those obligations required by applicable Data Protection Laws and Regulations.

6.3.1. Access to Third-Party Certifications and Audits Information. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Recognize shall:

(i) the make available to Customer (or Customer's Third-Party Auditor - as defined below in section 6.2.4) information regarding Recognize's compliance with the obligations set forth in this DPA in the form of a copy of Recognize's then most recent third-party audits or certifications set forth in the Security and Privacy Documentation. Such third-party audits or certifications may also be shared with Customer's competent supervisory authority on its request;

(ii) provide Customer with a report and/or confirmation of Recognize's audits of third-party Sub-processors' compliance with the data protection controls set forth in this DPA and/or a report of third-party auditors' audits of third party Subprocessors that have been provided by those third-party Sub-processors to Recognize, to the extent such reports or evidence may be shared with Customer ("Third-party Sub-processor Audit Reports"). Customer acknowledges that

(i) Third-party Sub-processor Audit Reports shall be considered Confidential Information as well as confidential information of the third-party Sub-processor and (ii) certain third-party Sub-processors to Recognize may require Customer to execute a non-disclosure agreement with them in order to view a Third-party Sub-processor Audit Report.

6.3.2. On-Site Audit. Customer can request an on-site audit of Recognize's Processing activities covered by this DPA ("On-Site Audit"). An On-Site Audit may be conducted by Customer either itself or through a Third-Party Auditor (as defined below in section 6.3.4) selected by Customer when:

(i) the information available pursuant to section "Third-Party Certifications and Audits" is not sufficient to demonstrate compliance with the obligations set out in this DPA and its Schedules;

(ii) Customer has received a notice from Recognize of a Customer Data Incident; or

(iii) such an audit is required by Data Protection Laws and Regulations or by Customer's competent supervisory authority.

Any On-Site Audits will be limited to Customer Data Processing and storage facilities operated by Recognize or any of Recognize's Affiliates.

6.3.3. Reasonable Exercise of Rights. An On-Site Audit shall be conducted by Customer or its Third-Party Auditor:

(i) acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Services used by Customer;

(ii) up to one time per year with at least three weeks' advance written notice. If an emergency justifies a shorter notice period, Recognize will use good faith efforts to accommodate the On-Site Audit request; and

(iii) during Recognize's normal business hours, under reasonable duration and shall not unreasonably interfere with Recognize's day-to-day operations. Before any On-Site Audit

commences, Customer and Recognize shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of Recognize. Recognize shall have the right to reasonably adapt the scope of any On-Site Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other Recognize customers' information.

6.3.4. Third-Party Auditor. A Third-Party Auditor means a third-party independent contractor that is not a competitor of Recognize. An On-Site Audit can be conducted through a Third Party Auditor if:

(i) prior to the On-Site Audit, the Third-Party Auditor enters into a non-disclosure agreement containing confidentiality provisions no less protective than those set forth in the Agreement to protect Recognize's proprietary information; and

(ii) the costs of the Third-Party Auditor are at Customer's expense.

6.3.5. Findings. Customer must promptly provide Recognize with information regarding any non-compliance discovered during the course of an On-Site Audit.

6.4. Data Protection Impact Assessment. Upon Customer's request, Recognize shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under Data Protection Laws and Regulations 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 Recognize.

## **7. CUSTOMER DATA INCIDENT MANAGEMENT**

Recognize maintains data security incident management and notification policies and procedures specified in the Security and Privacy Documentation and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Recognize or its Sub-processors of which Recognize becomes aware (a "Customer Data Incident").

Recognize shall make reasonable efforts to identify the cause of such Customer Data Incident and take such steps as Recognize deems necessary and reasonable to remediate the cause of such a Customer Data Incident to the extent the remediation is within Recognize's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

## **8. RETURN AND DELETION OF CUSTOMER DATA**

Recognize shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Security

and Privacy Documentation. Until Customer Data is deleted or returned, Recognize shall continue to comply with this DPA and its Schedules.

## **9. AUTHORIZED AFFILIATES**

9.1. Contractual Relationship. The parties acknowledge and agree that, by executing the Agreement, Customer enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Recognize and each such Authorized Affiliate subject to the provisions of the Agreement and this section 9 and section 10. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement.

For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is a party only to this DPA. All access to and use of the Services and Content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

9.2. Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Recognize under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.3. Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to this DPA with Recognize, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

9.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Recognize directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA, not separately for each Authorized Affiliate individually, but in a combined manner for itself and all of its Authorized Affiliates together (as set forth, for example, in section 9.3.2, below).

9.3.2 The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an On-Site Audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Recognize and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

## **10. LIMITATION OF LIABILITY**



Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Recognize, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, Recognize's and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

## **11. EUROPE SPECIFIC PROVISIONS**

11.1. Definitions. For the purposes of this section 12 and Schedule 1 these terms shall be defined as follows:

"European Personal Data" means the Personal Data subject to European Data Protection Laws and Regulations.

"European Data Protection Laws and Regulations" means the Data Protection Laws and Regulations applying in Europe.

"SCC Module 2" means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference

Module Two (Controller-to-Processor).

"Third-Country Transfer" means a transfer of European Personal Data that is not subject to an adequacy decision by the

European Commission. When US entities part of the Recognize Group or its Sub-processors are certified under the EU-US Data Privacy Framework and its extensions, the Parties agree that transfers to such entities are not considered Third-Country Transfers.

11.2. GDPR. Recognize will Process Personal Data in accordance with the GDPR requirements directly applicable to Recognize's provision of its Services.

11.3. Transfer mechanisms for data transfers. If, in the performance or use of the Services, European Personal Data is subject to a Third-Country Transfer, the transfer mechanisms listed below shall apply:

- SCC Module 2. Where Customer and/or its Authorized Affiliate is a Controller and a data exporter, subject to the additional terms in section 2 of Schedule 1; and/or

11.4. Impact of local laws. As of the Effective Date, Recognize has no reason to believe that the laws and practices in any third country of destination applicable to its Processing of the Personal Data as set forth in the Infrastructure and Sub-processors Documentation, including any requirements to disclose Personal Data or measures authorizing access by a Public Authority, prevent Recognize from fulfilling its obligations under this DPA. If Recognize reasonably believes that any existing or future enacted or enforceable laws and practices in the third country of destination applicable to its Processing of the Personal Data ("Local Laws") prevent it from fulfilling its obligations under this DPA, it shall promptly notify Customer. In such a case, Recognize shall use reasonable efforts to make available to the affected Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to facilitate compliance with the Local Laws without unreasonably burdening Customer. If Recognize is unable to make available such change promptly, Customer may terminate the applicable Order Form(s) and suspend the transfer of Personal Data in respect only to those Services which cannot be provided by Recognize in accordance with the Local Laws by providing written notice in accordance with the "Notices" section of the Agreement. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination for such terminated Services.

## **12. CANADA SPECIFIC PROVISIONS**

If Recognize processes Personal Data concerning persons located in Canada in the course of providing Services, Recognize agrees to the additional obligations and requirements in this section. Recognize shall not take any actions or make any omissions that may be in violation of the Personal Information Protection and Electronic Documents Act (PIPEDA), as amended or supplemented from time to time, and any other Canadian federal or provincial legislation governing the processing of Personal Data. Recognize shall keep all data, databases or other records containing Personal Data processed in connection with the Services logically isolated and separate from any information, data, databases or other records processed by Customer for itself or for third parties. Recognize has designated and identified its Chief Information Officer as an individual responsible for the oversight of the Personal Data. Recognize may be required to disclose, without advance notice or consent, Confidential Information of Customer to authorities in connection with any investigation, audit or inquiry in connection with the Services. Recognize shall not move, remove, or transmit any Personal Data from Customer's facilities without the express consent of Customer and without using appropriately secure technology to protect such information while in transit. If Recognize is contacted by a person with a request, inquiry or complaint regarding their Personal Data in connection with the Services, Recognize shall promptly refer such person to Customer.

## **13. AUSTRALIA SPECIFIC PROVISIONS**

The parties acknowledge that Recognize processes the Personal Data in Australia. Unless an adequacy decision exists for the respective locations, the Parties herewith agree to the EU Standard Contractual Clauses as set forth under Section 11.

Where the defined terms under Section 1 do not have application under Data Protection Laws and Regulations (e.g. Australian Data Privacy Laws), the parties' obligations will be interpreted to align as closely as possible with the scope of those roles and concepts under the GDPR while still fully complying with the applicable Data Protection Laws and Regulations.

“Australian Data Privacy Laws” means (i) the Privacy Act 1988 (Cth), including the ‘Australian Privacy Principles’ that form part of that Act; and (ii) all other laws applicable in respect of the processing of Personal Data.

### **List of Schedules**

Schedule 1: Transfer Mechanisms for European Data Transfers

Schedule 2: Description of Processing/Transfer

## **SCHEDULE 1 - TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS**

### **1. STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS**

For the purpose of SCC Module 2, Customer is the data exporter and Recognize Services, Inc is the data importer and the Parties agree to the following. Where the Recognize entity that is a party to this DPA is not Recognize Inc, that Recognize entity is carrying out the obligations of the data importer on behalf of Recognize Inc. If and to the extent an Authorized Affiliate relies on SCC Module 2 for the transfer of Personal Data, any references to “Customer” in this Schedule, include such Authorized Affiliate.

1.1. Reference to the Standard Contractual Clauses. The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Schedule 2.

1.2. Docking clause. The option under clause 7 shall not apply.

1.3. Instructions. This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to Recognize for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of clause 8.1(a), the instructions by Customer to Process Personal Data are set out in section 2.2 of this DPA and include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.

1.4. Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Recognize to Customer only upon Customer's written request.

1.5. Security of Processing. For the purposes of clause 8.6(a), Customer is responsible for making an independent determination as to whether the technical and organizational measures set forth in the Security and Privacy Documentation meet Customer's requirements and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by Recognize provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of clause 8.6(c), personal data breaches will be handled in accordance with section 7 (Customer Data Incident Management and Notification) of this DPA.

1.6. Audits of the SCCs. The parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with section 6.3 of this DPA.

1.7. General authorization for use of Sub-processors. Option 2 under clause 9 shall apply. For the purposes of clause 9(a), Recognize has Customer's general authorization to engage Sub-processors in accordance with section 5 of this DPA. Recognize shall make available to Customer the current list of Sub-processors in accordance with section 5.2 of this DPA.

1.8. Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to clause 9(a), Customer acknowledges and expressly agrees that Recognize may engage new Sub-processors as described in sections 5.2 and 5.3 of this DPA. Recognize shall inform Customer of any changes to Sub-processors following the procedure provided for in section 5.2 of this DPA.

1.9. Complaints - Redress. For the purposes of clause 11, and subject to section 3 of this DPA, Recognize shall inform data subjects on its website of a contact point authorized to handle complaints. Recognize shall inform Customer if it receives a complaint by, or a dispute from, a Data Subject with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Customer. Recognize shall not otherwise have any obligation to handle the request (unless otherwise agreed with Customer). The option under clause 11 shall not apply.

1.10. Supervision. Clause 13 shall apply as follows:

1.10.1. Where Customer is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Customer with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

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

1.10.3. Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, Commission nationale de l'informatique et des libertés (CNIL) - 3 Place de Fontenoy, 75007 Paris, France shall act as competent supervisory authority.

1.10.4. Where Customer is established in the United Kingdom or falls within the territorial scope of application of the Data Protection Laws and Regulations of the United Kingdom ("UK Data Protection Laws and Regulations"), the Information Commissioner's Office ("ICO") shall act as competent supervisory authority.

1.10.5. Where Customer is established in Switzerland or falls within the territorial scope of application of the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws and Regulations"), the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

1.11. Notification of Government Access Requests. For the purposes of clause 15(1)(a), Recognize shall notify Customer (only) and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.

1.12. In Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law.

1.13. In Clause 18(b), disputes will be resolved before the courts of Ireland.

1.14. Appendix. The Appendix shall be completed as follows:

- The contents of section 1 of Schedule 2 shall form Annex I.A to the Standard Contractual Clauses
- The contents of sections 2 to 9 of Schedule 2 shall form Annex I.B to the Standard Contractual Clauses
- The contents of section 10 of Schedule 2 shall form Annex I.C to the Standard Contractual Clauses
- The contents of section 11 of Schedule 2 to this Exhibit shall form Annex II to the Standard Contractual Clauses.

1.15. Data Exports from the United Kingdom under the Standard Contractual Clauses. For data transfers governed by UK Data Protection Laws and Regulations, the 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 revised under Section 18 of those Mandatory Clauses ("Approved Addendum") shall apply. The information required for Tables 1 to 3 of Part One of the Approved Addendum is set out in Schedule 2 of this DPA (as applicable). For the purposes of Table 4 of Part One of the Approved Addendum, neither party may end the Approved Addendum when it changes.

1.16. Data Exports from Switzerland under the Standard Contractual Clauses. For data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity. In such circumstances, general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in Swiss Data Protection Laws.

1.17. Conflict. The Standard Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

## SCHEDULE 2 - DESCRIPTION OF PROCESSING/TRANSFER

### 1. LIST OF PARTIES

Data exporter(s): Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Agreement and as further described in the Documentation.

Signature and date:

Role: For the purposes of SCC Module 2 Customer and/or its Authorized Affiliate is a Controller.

Data importer(s): Identity and contact details of the data importer(s), including any contact person with responsibility for data protection

Name: Recognize Services, Inc.

Address: 760A Gilman Street, Berkeley, CA 94710

Contact person's name, position and contact details: Peter Philips

Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Agreement and as further described in the Documentation.

Signature and date: 

Role: Processor

### 2. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

Customers' employees

### **3. CATEGORIES OF PERSONAL DATA TRANSFERRED**

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Display name
- Email address
- IP address
- Name of Employer
- Hire date
- Birthday
- Phone number

### **4. SENSITIVE DATA TRANSFERRED (IF APPLICABLE)**

None

### **5. FREQUENCY OF THE TRANSFER**

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

Continuous basis depending on the use of the Services by Customer.

### **6. NATURE OF THE PROCESSING**

The nature of the Processing is the performance of the Services pursuant to the Agreement.

### **7. PURPOSE OF PROCESSING, THE DATA TRANSFER AND FURTHER PROCESSING**

Recognize will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services.



## **8. DURATION OF PROCESSING**

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Subject to section 9 of the DPA, Recognize will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

## **9. SUB-PROCESSOR TRANSFERS**

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

As per 7 above, the Sub-processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement.

Subject to section 9 of this DPA, the Sub-processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

Identities of the Sub-processors used for the provision of the Services and their country of location are listed at <https://recognizeapp.com/gdpr/recognize-subprocessors.pdf>

## **10. COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with clause 13: the supervisory authority specified in section 2.10 of Schedule 1 shall act as the competent supervisory authority.

## **11. TECHNICAL AND ORGANISATIONAL MEASURES**

Recognize will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Security and Privacy Documentation applicable to the specific Services purchased by Customer. Recognize will not materially decrease the overall security of the Services during a subscription term.