ESKALERA DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements the master agreement (the "**MSA**") entered into by and between you and the organization you represent ("**Customer**") and Eskalera, Inc. ("**Eskalera**"). This DPA incorporates the terms of the MSA, and any terms not defined in this DPA shall have the meaning set forth in the MSA.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. Capitalized terms not otherwise defined herein shall have the meaning given to them in the MSA. Reference to the MSA in this DPA includes any Order Form subject to the MSA (including any such Order Form entered into in the future). Except as modified below, the terms of the MSA shall remain in full force and effect. This DPA shall be effective for the duration of the MSA (or longer to the extent required by applicable law).

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 MSA, but has not signed its own Order Form with Eskalera and is not a "Customer" as defined under this DPA.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Data Protection Laws**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement as amended from time to time.

"**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**" shall have the meaning ascribed to "personally identifiable information," "personal information," "personal data" or equivalent terms as such terms are defined under the Data Protection Laws, in each case that is Company Data under the MSA.

"**Processing**" or "**Process**" means any operation or set of operations that is performed on 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 that Processes Personal Data on behalf of the Controller.

"**Public Authority**" means a government agency or law enforcement authority, including judicial authorities.

"**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://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

"**Sub-processor**" means any entity appointed by Eskalera to Process Personal Data on behalf of Customer.

2. **PROCESSING OF PERSONAL DATA**

2.1. **Roles of the Parties**. The parties acknowledge and agree that regarding the Processing of Personal Data under the MSA, Customer is the Controller (or a Processor), Eskalera is the Processor and Eskalera will engage Sub-processors pursuant to Section 5 below.

2.2. **Customer's Processing of Personal Data**. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws, including any applicable requirement to provide notice to Data Subjects of the use of Eskalera as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. 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.

2.3. **Eskalera's Processing of Personal Data**. Eskalera shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions unless Processing is required by Data Protection Laws. Customer instructs Eskalera (and authorizes Eskalera to instruct each Sub-processor) to Process Personal Data for the following purposes: (i) Processing in accordance with the MSA; (ii) Processing initiated by Customer's users in their use of the Services; or (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 MSA.

2.4. **Details of the Processing**. The subject matter of Processing of Personal Data by Eskalera is the performance of the Services pursuant to the MSA. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and the categories of Data Subjects Processed under this DPA are further specified in Schedule 2.

3. **RIGHTS OF DATA SUBJECTS**

3.1. Eskalera shall, to the extent legally permitted, promptly notify Customer of any complaint, dispute or request it has received from a Data Subject regarding the Processing of its Personal Data, 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". Eskalera shall not respond to a Data Subject Request itself, except that Customer authorizes Eskalera to redirect the Data Subject Request as necessary to allow Customer to respond directly. Taking into account the nature of the Processing, Eskalera shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Eskalera shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Eskalera is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Eskalera's provision of such assistance.

4. **ESKALERA PERSONNEL**

4.1. **Confidentiality**. Eskalera 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. Eskalera shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. **Reliability**. Eskalera shall take commercially reasonable steps to ensure the reliability of any Eskalera personnel engaged in the Processing of Personal Data.

4.3. **Limitation of Access**. Eskalera shall ensure that Eskalera's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5. SUB-PROCESSORS

5.1. **Appointment of Sub-processors**. Customer acknowledges and agrees that (a) Eskalera's Affiliates may be retained as Sub-processors; and (b) Eskalera and Eskalera's Affiliates may engage Sub-processors in connection with provision of the Services. Eskalera (or its Affiliate) shall enter into a written agreement with any engaged Sub-processor that contains data protection obligations no less protective than those contained in this DPA 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. **List of Current Sub-processors and Notification of New Sub-processors**. A current list of Sub-processors for the Services, including the identities of those Sub-processors and their country of location, may be requested at any time by emailing dpa@eskalera.com. Customer may receive notifications of new Sub-processors by emailing dpa@eskalera.com with the subject "Subscribe", and if a Customer contact subscribes, Eskalera shall provide the subscriber with notification of new Sub-processor(s) before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

5.3. **Objection to New Sub-processors**. Customer may object to Eskalera's use of a new Sub-processor by notifying Eskalera in writing within ten (10) business days after receipt of Eskalera's communication advising of the new Sub-processor. In the event Customer reasonably objects to the use of a new Sub-processor as permitted in the prior sentence, Eskalera 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 Eskalera is unable to make available such change within a reasonable period, which shall not exceed ninety (90) days, Customer may terminate the applicable Order Form with respect only to those Services which cannot be provided by Eskalera without the use of the objected-to new Sub-processor by providing written notice to Eskalera. Eskalera will refund Customer any prepaid fees covering the remainder of the term of such Order Form following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

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

6. SECURITY

6.1. **Controls for the Protection of Personal Data**. Eskalera 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, Personal Data), confidentiality and integrity of Personal Data. Eskalera regularly monitors compliance with these measures. Eskalera will not materially decrease the overall security of the Services during a subscription term.

6.2. **Audit**. Eskalera shall maintain an audit program to help ensure compliance with the obligations set out in this DPA and shall make available to Customer information to demonstrate compliance with the obligations set out in this DPA as set forth in this Section 6.2.

6.2.1. **Third-party Certifications and Audits**. Eskalera has obtained the third-party certifications and audits for the Services. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Eskalera shall make available to Customer (or Customer's Third-party Auditor - as defined below in Section 6.2.4) information regarding Eskalera's compliance with the obligations set forth in this DPA. Where Eskalera has obtained ISO 27001 certifications and SSAE 18 Service Organization Control (SOC) 2 reports for the Services, Eskalera agrees to maintain these certifications or standards, or appropriate and comparable successors thereof, for the duration of the Agreement. Upon request, Eskalera shall also provide a requesting Customer with a report and/or confirmation of Eskalera'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 Sub-processors that have been provided by those third-party Sub-processors to Eskalera, 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 Eskalera may require Customer to execute a non-disclosure agreement with them in order to view a Third-party Sub-processor Audit Report.

6.2.2. **On-Site Audit**. Customer may contact Eskalera to request an on-site audit of Eskalera'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 6.2.4) selected by Customer when:

(i) the information available pursuant to Section 6.2.1 is not sufficient to demonstrate compliance with the obligations set out in this DPA and its Schedules;

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

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

Any On-Site Audits will be limited to Personal Data Processing and storage facilities operated by Eskalera or any of Eskalera's Affiliates. Customer acknowledges that Eskalera operates a multi-tenant cloud environment. Accordingly, Eskalera 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 Eskalera customers' information.

6.2.3. **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, Eskalera will use good faith efforts to accommodate the On-Site Audit request; and

(iii) during Eskalera's normal business hours, under reasonable duration and shall not unreasonably interfere with Eskalera's day-to-day operations.

Before any On-Site Audit commences, Customer and Eskalera 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 Eskalera.

6.2.4. **Third-party Auditor**. A Third party Auditor means a third-party independent contractor that is not a competitor of Eskalera. 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 Eskalera's proprietary information; and

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

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

6.3. **Data Protection Impact Assessment**. Upon Customer's request, Eskalera shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Data Protection Laws 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 Eskalera.

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

7.1. Eskalera maintains security incident management policies and procedures and 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 transmitted, stored or otherwise Processed by Eskalera or its Sub-processors of which Eskalera becomes aware (a "**Customer Data Incident**"). Eskalera shall make reasonable efforts to identify the cause of such Customer Data Incident and take such steps as Eskalera deems necessary and reasonable to remediate the cause of such a Customer Data Incident to the extent the remediation is within Eskalera's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users.

8. GOVERNMENT ACCESS REQUESTS.

8.1. **Eskalera requirements**. In its role as a Processor, Eskalera shall maintain appropriate measures to protect Personal Data in accordance with the requirements of Data Protection Laws, including by implementing appropriate technical and organizational safeguards to protect Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defense and public security. If Eskalera receives a legally binding request to access Personal Data from a Public Authority, Eskalera shall, unless otherwise legally prohibited, promptly notify Customer including a summary of the nature of the request. To the extent Eskalera is prohibited by law from providing such notification, Eskalera shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable Eskalera to communicate as much information as possible, as soon as possible. Further, Eskalera shall challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. Eskalera shall pursue possibilities of appeal. When challenging a request, Eskalera shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. Eskalera agrees it will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. Eskalera shall promptly notify Customer if Eskalera becomes aware of any direct access by a Public Authority to Personal Data and provide information available to Eskalera in this respect, to the extent permitted by law. For the avoidance of doubt, this DPA shall not require Eskalera to pursue action or inaction that could result in civil or criminal penalty for Eskalera such as contempt of court.

8.2. **Sub-processors requirements**. Eskalera shall ensure that Sub-processors involved in the Processing of Personal Data are subject to the relevant commitments regarding Government Access Requests in the Standard Contractual Clauses.

9. RETURN AND DELETION OF PERSONAL DATA

9.1. Eskalera shall, upon Customer's written request, promptly destroy or return any Personal Data after the end of the provision of Services, unless storage of the Personal Data is required by applicable law.

10. AUTHORIZED AFFILIATES

10.1. **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 Eskalera and each such Authorized Affiliate subject to the provisions of the Agreement. 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 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.

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

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

10.3.1. Except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Eskalera 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 10.3.2, below).

10.3.2. 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 Eskalera 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.

11. LIMITATION OF LIABILITY

11.1. 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 Eskalera, whether in contract, tort or under any other theory of liability, is subject to any limitations of liability provision(s) set forth in the MSA, 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, Eskalera'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.

12. EUROPE SPECIFIC PROVISIONS

12.1. **Definitions**. For the purposes of this Section 12 and Schedule 1 these terms shall be defined as follows:

"**EU C-to-P Transfer Clauses**" means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor).

"**EU P-to-P Transfer Clauses**" means Standard Contractual Clauses sections I, II III and IV (as applicable) to the extent they reference Module Three (Processor-to-Processor).

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

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

12.4. **Transfer mechanisms for data transfers**. If, in the performance of the Services, Personal Data that is subject to the GDPR or any other law relating to the protection or privacy of individuals that applies in Europe is transferred out of Europe to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws of Europe, the transfer mechanisms listed below shall apply to such transfers and can be directly enforced by the parties to the extent such transfers are subject to the Data Protection Laws of Europe:

- The EU C-to-P Transfer Clauses. Where Customer and/or its Authorized Affiliate is a Controller and a data exporter of Personal Data and Eskalera is a Processor and data importer in respect of that Personal Data, then the parties shall comply with the EU C-to-P Transfer Clauses, subject to the additional terms in Section 1 of Schedule 1; and/or
- The EU P-to-P Transfer Clauses. Where Customer and/or its Authorized Affiliate is a Processor acting on behalf of a Controller and a data exporter of Personal Data and Eskalera is a Processor and data importer in respect of that Personal Data, the parties shall comply with the terms of the EU P-to-P Transfer Clauses, subject to the additional terms in Sections 1 and 2 of Schedule 1.

12.5. **Impact of local laws**. As of the Effective Date, Eskalera has no reason to believe that the laws and practices in any third country of destination applicable to its Processing of the Personal Data, including any requirements to disclose Personal Data or measures authorising access by a Public Authority, prevent Eskalera from fulfilling its obligations under this DPA. If Eskalera 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, Eskalera 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 Eskalera 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 Eskalera in accordance with the Local Laws by providing written notice in accordance with the notice provisions of the MSA. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination for such terminated Services.

<u>List of Schedules</u>

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 purposes of the EU C-to-P Transfer Clauses and the EU P-to-P Transfer Clauses, Customer is the data exporter and Eskalera is the data importer and the parties agree to the following. If and to the extent an Authorized Affiliate relies on the EU C-to-P Transfer Clauses or the EU P-to-P Transfer Clauses for the transfer of Personal Data, any references to 'Customer' in this Schedule, include such Authorized Affiliate. Where this Section 1 does not explicitly mention EU C-to-P Transfer Clauses or EU P-to-P Transfer Clauses it applies to both of them.

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 MSA are Customer's documented instructions at the time of signature of the Agreement to Eskalera for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the MSA. For the purposes of clause 8.1(a), the instructions by Customer to Process Personal Data are set out in Section 2.3 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 Eskalera to Customer only upon Customer's written request.

1.5. **Security of Processing**. For the purposes of clause 8.6(a), Customer is solely responsible for making an independent determination as to whether the technical and organisational measures Eskalera employs 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 Eskalera 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 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 6.2 of this DPA.

1.7. **General authorisation for use of Sub-processors**. Option 2 under clause 9 shall apply. For the purposes of clause 9(a), Eskalera has Customer's general authorisation to engage Sub-processors in accordance with Section 5 of this DPA. Eskalera shall make available to Customer the current list of Sub-processors in accordance with section 5.2 of this DPA. Where Eskalera enters into the EU P-to-P Transfer Clauses with a Sub-processor in connection with the provision of the Services, Customer hereby grants Eskalera and Eskalera's Affiliates authority to provide a general authorisation on Controller's behalf for the engagement of sub-processors by Sub-processors engaged in the provision of the Services, as well as decision making and approval authority for the addition or replacement of any such sub-processors.

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 Eskalera may engage new Sub-processors as described in sections 5.2 and 5.3 of this DPA. Eskalera 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, Eskalera shall inform data subjects on its website of a contact point authorised to handle complaints. Eskalera 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. Eskalera 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. **Liability**. Eskalera's liability under clause 12(b) shall be limited to any damage caused by its Processing where Eskalera has not complied with its obligations under the GDPR specifically directed to Processors, or where it has acted outside of or contrary to lawful instructions of Customer, as specified in Article 82 GDPR.

1.11. **Supervision**. Clause 13 shall apply as follows:

1.11.1. 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.

1.11.2. 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.

1.11.3. 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.

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

1.11.5. Where Customer is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws, 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.

1.12. **Notification of Government Access Requests**. For the purposes of clause 15(1)(a), Eskalera 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.

1.13. **Governing Law**. The governing law for the purposes of clause 17 shall be the law that is designated in the Governing Law section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of France; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of the United Kingdom.

1.14. **Choice of forum and jurisdiction**. The courts under clause 18 shall be those designated in the applicable section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree that the courts of either (i) France; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the United Kingdom, shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

1.15. **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.

1.16. **Data Exports from the United Kingdom and Switzerland under the Standard Contractual Clauses**. In case of any transfers of Personal Data from the United Kingdom and/or transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws of Switzerland (“**Swiss Data Protection Laws**”), (i) 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 the Data Protection Laws of the United Kingdom (“**UK Data Protection Laws**”) or Swiss Data Protection Laws, as applicable; and (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Data Protection Laws or Swiss Data Protection Laws, as applicable. In respect of 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.

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.

2. ADDITIONAL TERMS FOR THE EU P-TO-P TRANSFER CLAUSES

For the purposes of the EU P-to-P Transfer Clauses (only), the parties agree the following.

2.1. **Instructions and notifications**. For the purposes of clause 8.1(a), Customer hereby informs Eskalera that it acts as Processor under the instructions of the relevant Controller in respect of Personal Data. Customer warrants that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to Eskalera for the appointment of Sub-processors in accordance with this DPA, have been authorized by the relevant Controller. Customer shall be solely responsible for forwarding any notifications received from Eskalera to the relevant Controller where appropriate.

2.2. **Security of Processing**. For the purposes of clause 8.6(c) and (d), Eskalera shall provide notification of a personal data breach concerning Personal Data Processed by Eskalera to Customer.

2.3. **Documentation and Compliance**. For the purposes of clause 8.9, all enquiries from the relevant Controller shall be provided to Eskalera by Customer. If Eskalera receives an enquiry directly from a Controller, it shall forward the enquiry to Customer and Customer shall be solely responsible for responding to any such enquiry from the relevant Controller where appropriate.

2.4. **Data Subject Rights**. For the purposes of clause 10 and subject to section 3 of this DPA, Eskalera shall notify Customer about any request it has received directly from a Data Subject without obligation to handle it (unless otherwise agreed), but shall not notify the relevant Controller. Customer shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.

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: Customer and its Authorized Affiliates.

Address: See order form (or such address as Customer may update to Eskalera on notice at any time).

Contact person's name, position and contact details: See order form (or such name as Customer may update to Eskalera on notice at any time).

Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Agreement.

Role: For the purposes of the EU C-to-P Transfer Clauses Customer and/or its Authorized Affiliate is a Controller. For the purposes of the EU P-to-P Transfer Clauses Customer and/or its Authorized Affiliate is a Processor.

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

Name: Eskalera, Inc.

Address: 23 Geary Street, Suite 600, San Francisco, CA 94108

Contact person's name, position and contact details: Rich Kneece, CTO; privacy@eskalera.com

Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Agreement.

Role: Processor

2. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED

Customer may submit Personal Data to Eskalera, the extent of which is determined and controlled by Customer in its sole discretion. This may include, but is not limited to Personal Data relating to the following categories of data subjects: Customer's employees, users, clients, agents and subcontractors.

3. CATEGORIES OF PERSONAL DATA TRANSFERRED

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

- Personal Data related to or relevant to the employment of Customer personnel
- Business contact details of Customers, Suppliers and Contractors (name, title/position, address, telephone number, fax number, email address, location)
- Connection data (IP address, username, ID data used for authentication purposes)

4. SENSITIVE DATA TRANSFERRED (IF APPLICABLE)

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

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

Eskalera will Process Personal Data as necessary to perform the Services pursuant to the Agreement, 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, Eskalera 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.

10. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with clause 13:

- Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.
- Where the data exporter 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 the competent supervisory authority.
- Where the data exporter 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 the competent supervisory authority.
- Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as the competent supervisory authority.
- Where the data exporter is established in Switzerland or falls within the territorial scope of application of 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.

11. TECHNICAL AND ORGANISATIONAL MEASURES

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services. Data Importer will not materially decrease the overall security of the Services during a subscription term. Data Subject Requests shall be handled in accordance with Section 3 of the DPA.