

Master Services Agreement

This Master Services Agreement ("**MSA**") is entered by and between Dataloop Ltd. ("**Dataloop**") and the customer identified on the order form referencing this MSA ("**Customer**" and "**Order Form**", respectively) as of the Effective Date set forth in the Order Form. This MSA, together with the Order Form, set forth the terms under which the Customer and its dedicated personnel ("**Employee(s)**") can use Dataloop's data management, data annotation and turn-key data labeling platform ("**Platform**") and the services provided through the Platform ("**Services**").

In the event of a conflict between an Order Form and this MSA, the provisions of the Order Form shall prevail to the extent of such conflict.

1. Services

- 1.1. During the Term (as defined below), Dataloop shall provide Customer and its Employees with a limited, revocable, non-exclusive, non-transferrable right to use the Platform and the Services, solely for Customer's internal business uses, and other uses, as detailed in the Order Form.
- 1.2. Dataloop shall use commercially reasonable efforts to provide Customer with technical support via email and to respond to all helpdesk tickets within one (1) Business Day during Business Hours. "**Business Day/s**" shall mean days on which the financial markets in Israel are open. "**Business Hours**" shall mean between 9:00-17:00 on Business Days.

2. Restrictions.

- 2.1. Customer shall not and shall not allow any Employee or any third party to (attempt) to (a) decipher, decompile, disassemble, or reverse-engineer any of the software used to provide the Platform, and/or Services; (b) circumvent, disable, or otherwise interfere with features of the Platform and/or Services related to security or access; (c) use any robot, spider, search or retrieval application, or any other manual or automatic device or process to retrieve, index, data-mine, or in any way reproduce or circumvent the navigational structure or presentation of the Platform and/or Services; or (d) harvest, collect or mine information about users of the Platform and Services. Except as expressly permitted herein, Customer may not and may not allow any third party to copy, modify, duplicate, distribute, display, perform, sublicense, republish, retransmit, reproduce, create derivative works of, transfer, sell, further develop, download, or otherwise use the Platform or Services or any content thereon or use the Platform or content thereon in any manner not permitted by this MSA. Customer will not remove, alter or conceal any copyright, trademark, service mark or other proprietary rights notices incorporated in the Platform or Services.
- 2.2. Customer shall not and shall not allow any Employee to transmit, submit or upload any materials to the Platform ("**Customer Materials**") or act in any way that: (1) restricts or inhibits use of the Platform or Services; (2) violates or results in the violation of the legal rights of others including their intellectual property rights, moral rights, publicity, privacy, or other rights; (4) is (or Customer reasonably believes or should reasonably believe to be) stolen, illegal, counterfeit, fraudulent, pirated, unauthorized, or in furtherance of any illegal, counterfeiting, fraudulent,

pirating, or unauthorized activity, or that involves (or Customer reasonably believes or should reasonably believe to involve) any stolen, illegal, counterfeit, fraudulent, pirated, or unauthorized material; (5) does not comply with all applicable laws, rules and regulations; (6) imposes an unreasonably or disproportionately large load on our infrastructure; or (7) posts, stores, transmits, or contains links to any virus, worm, trojan horse, or other harmful or disruptive component or anything that violates any law or regulation.

3. Consideration.

- 3.1. In consideration of the use of the Platform and the Services, Customer shall pay Dataloop the applicable fees set forth in the Order Form ("**Fees**") in accordance with the plan selected by the Customer ("**Plan**") and the payment terms set forth therein. If Customer's use of the Services exceeds the Service Capacity set forth on the Order Form or otherwise requires the payment of additional fees (per the terms of this MSA), Customer shall be billed for such usage and Customer agrees to pay the additional fees in the manner provided herein. In the event that the Customer wishes to upgrade the chosen Plan to a Plan with a higher service capacity, Customer shall provide seven (7) days' prior written notice of the requested change. Once a Plan has been upgraded, the terms of the upgraded Plan shall apply for the remainder of the Term, unless upgraded further. It is clarified that Plans may not be downgraded to a lower service capacity.
- 3.2. Late payments shall bear interest at the rate of 12% per annum.
- 3.3. Dataloop reserves the right to change the Fees or applicable charges and to institute new charges and Fees at the end of the Initial Term or then-current Renewal Term (both as identified in the Order Form), upon thirty (30) days prior notice to Customer (including by email).

4. Representations and Warranties

- 4.1. Each party hereby represents and warrants that (a) it is a duly organized under applicable law; (b) it has the authority to enter into this Agreement; (c) the execution and performance of this Agreement does not conflict with any contractual obligations it has to any third party or legal requirement. Customer further represents and warrants that: (i) any Customer Materials do not and will not infringe the intellectual property, privacy, publicity or moral rights of any third party; (ii) it has all rights, licenses, and consents necessary to provide such Customer Materials to Dataloop; and (iii) it shall at all times use the Platform and Services in compliance with applicable law.
- 4.2. With respect to Personal Data (as defined in the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**")) that is included in Customer Materials, Customer represents and warrants that (i) it shall be considered a Controller (as defined in the GDPR) of such Personal Data; (ii) it has provided any and all notices and has and shall maintain throughout the Term all necessary rights and consents required under applicable law to provide Personal Data to Dataloop in order to allow it to provide its Services hereunder; (iii) it shall neither provide Dataloop with, nor grant it access to, any Personal Data unless such notices and consents have lawfully been provided or obtained, as

applicable; and (iv) it shall ensure that a record of such consents is maintained, as required under applicable law. The parties shall enter into the Data Processing Agreement attached hereto as **Schedule A ("DPA")** and which is an integral part of this Agreement. In case of any conflict between the Agreement and the DPA, the provisions of the DPA shall prevail to the extent of such inconsistency.

5. Intellectual Property

- 5.1. Dataloop IP. Dataloop and its licensors, as the case may be, own all rights, title, and interest in and to the Platform, Services and all software and technical innovations providing the Platform and Services, as well as in all modifications, enhancements, and updates thereto and all worldwide intellectual property rights, and the trademarks, service marks, and logos contained therein whether registered and unregistered. Customer may not remove, alter or conceal any copyright, trademark, service mark or other proprietary rights notices incorporated in the Platform or other materials, if any. All trademarks are trademarks or registered trademarks of their respective owners. Nothing in this MSA grants Customer any right to use any trademark, service mark, logo, or trade name of Dataloop or any third party. Nothing in this MSA shall be interpreted to provide Customer with any rights in the Platform or Services except the limited right to use the Platform and to receive the Services subject to the terms and conditions hereof. If Customer or its Employees provide Dataloop with any feedback regarding the Platform or Services, Dataloop may use all such feedback without restriction and shall not be subject to any non-disclosure or non-use obligations in respect of such feedback.
- 5.2. Customer Materials. Customer shall own all right, title and interest in and to any materials it uploads to the Platform ("**Customer Materials**") and any materials generated by the Platform based on the Customer Materials.
- 5.3. License. Customer hereby grants Dataloop and its successors and assignees, as well as its service providers, a worldwide, royalty-free, fully paid-up and non-exclusive license under any of Customer's intellectual property, moral or privacy rights to use, copy, distribute, display, modify and create derivative works of any Customer Materials solely for the provision of the Services in accordance with the terms of this Agreement and during the Term of this Agreement.

6. Confidential and Proprietary Information.

- 6.1. Confidential Information. Each party (each, a "**Recipient**") may have access to certain non-public or proprietary information of the other party (each, a "**Disclosing Party**") including any technical or non-technical information related to the other party's business and current, future and proposed products, services, and (prospective) customers in each case whether or not specifically designated as "confidential" or "proprietary" ("**Confidential Information**"). The terms of this Agreement shall be considered the Confidential Information of Dataloop.
- 6.2. Nondisclosure Obligations. Except as permitted herein, Recipient may not use, disseminate, or in any way disclose the Confidential Information except for purposes of providing or receiving the Services or in furtherance of the relationship of the parties hereunder. Recipient may use the Confidential Information solely for the purposes set out in this Agreement. Recipient shall treat all Confidential Information

with the same degree of care as it accords to its own Confidential Information but in any event with a high degree of care. Recipient shall disclose Confidential Information only to those of its employees who have a need to know the information in order for Recipient to perform its obligations under this Agreement and which are bound by non-disclosure and non-use obligations no less restrictive than those set out herein. The obligations set forth in this section shall survive termination of this Agreement for any reason.

- 6.3. Exclusions. Recipient's obligations hereunder do not apply to any Confidential Information that Recipient can demonstrate by written records (a) was in the public domain at or subsequent to the time the Confidential Information and was received by Recipient through no act or omission of Recipient; (b) was rightfully in Recipient's possession free of any obligation of confidence at or subsequent to the time the Confidential Information was communicated to Recipient by Disclosing Party; or (c) was independently developed by Recipient without use of, or reference to, any Confidential Information. A disclosure of any Confidential Information by Recipient in response to a law, regulation, or governmental or judicial order ("**Order**") will not be considered to be a breach of this Agreement or a waiver of confidentiality for other purposes; provided, however, that Recipient, to the extent permitted by such Order (a) provides prompt prior written notice thereof to Disclosing Party of such Order; (b) reasonably cooperates with Disclosing Party in opposing such disclosure, (c) only discloses to extent required by such Order.

7. **Indemnification.**

- 7.1. By Customer. Customer shall defend, indemnify and hold harmless Dataloop (and its officers, directors and employees) from and against any and all damages, costs, losses, liabilities or expenses (including court costs and reasonable attorneys' legal fees) that Dataloop may suffer or incur in connection with any actual or threatened claim, demand, action or other proceeding by any third party arising from or relating to (i) any breach of this Agreement by the Customer, its Employees, or anyone on its behalf; (ii) use or misuse of the Platform and/or Services; (iii) infringement of a third party's intellectual property or other rights, including but not limited to the Customer Materials; or (iv) the Customer Materials. Customer may not settle or compromise such suit without the written consent of Dataloop. Dataloop may be represented in any such suit by counsel of its own choosing at its own expense.
- 7.2. By Dataloop. Dataloop shall defend, indemnify and hold harmless Customer (and its officers, directors and employees) from and against any and all damages, costs, losses, liabilities or expenses (including court costs and reasonable attorneys' legal fees) that Customer may suffer or incur in connection with any actual or threatened claim, demand, action or other proceeding by any third party arising from or relating to a claim that the Platform or Services, as delivered, infringes any patent or copyright, provided however, that Dataloop shall have no responsibility or liability for any claim to the extent resulting from or arising out of (a) the use of the Platform or Services not in compliance with this Agreement or applicable law; (b) the combination of the Platform or Services with any services not provided by Dataloop; or (c) the modification of any Platform or Services by any party other than Dataloop. Customer may not settle or compromise such suit without the written consent of Dataloop. Dataloop may be represented in any such suit by counsel of its own choosing at its own expense.

8. Disclaimer of Warranty.

8.1. Dataloop shall use reasonable efforts to maintain the Platform and Services in a manner which minimizes errors and interruptions. However, access to the Platform and/or Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Dataloop or by third-party providers, or due to other causes beyond Dataloop's reasonable control. Dataloop shall use reasonable efforts to provide notice in writing or by e-mail of any scheduled service disruption. However, Dataloop does not warrant that the Services will be uninterrupted or error free; nor does it make any warranty as to the results that may be obtained from use of the Services.

8.2. THE PLATFORM AND SERVICES ARE PROVIDED ON AN "AS-IS" AND "AS AVAILABLE" BASIS. EXCEPT AS SPECIFICALLY SET FORTH HEREIN, DATALOOP EXPRESSLY DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS IN RESPECT OF THE PLATFORM AND SERVICES INCLUDING, WITHOUT LIMITATION, EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

8.3. CUSTOMER HEREBY ACKNOWLEDGES THAT DATALOOP DOES NOT MONITOR CUSTOMER MATERIALS FOR INAPPROPRIATE, ILLEGAL AND/OR ANY OTHER MATERIALS AND THAT CUSTOMER SHALL BE SOLELY RESPONSIBLE FOR ANY CONSEQUENCES RESULTING FROM THE CUSTOMER MATERIALS UPLOADED TO THE PLATFORM. CUSTOMER SHALL BE SOLELY RESPONSIBLE IN THE EVENT THAT ITS EMPLOYEES OR ANY OTHER USERS ON THE PLATFORM ARE EXPOSED TO MATERIALS WITHIN THE CUSTOMER MATERIALS THAT ARE (A) OFFENSIVE (INCLUDING MATERIAL PROMOTING OR GLORIFYING HATE, VIOLENCE, BIGOTRY, OR ENTITIES DEDICATED TO OR ASSOCIATED WITH SUCH CAUSES); (B) MATERIAL THAT IS RACIALLY OR ETHNICALLY INSENSITIVE, MATERIAL THAT IS DEFAMATORY, HARASSING OR THREATENING; (C) PORNOGRAPHY OR OBSCENE MATERIAL; AND/OR (D) MATERIAL THAT IS OTHERWISE INAPPROPRIATE OR OFFENSIVE. DATALOOP SHALL HAVE NO LIABILITY IN CONNECTION WITH THE FOREGOING.

9. **LIMITATION OF LIABILITY.** IN NO EVENT SHALL DATALOOP OR ITS DIRECTORS, OFFICERS, EMPLOYEES, AGENTS, OR CONSULTANTS, HAVE ANY LIABILITY FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL OR PUNITIVE DAMAGES, ARISING OUT OF OR RELATING TO THE PLATFORM OR SERVICES OR THE ARRANGEMENTS CONTEMPLATED HEREIN, INCLUDING IN RESPECT OF LOST PROFITS, LOST BUSINESS OPPORTUNITIES, OR LOST DATA. DATALOOP'S MAXIMUM CUMULATIVE LIABILITY UNDER THIS AGREEMENT AND/OR ANY CAUSE OF ACTION IS LIMITED TO THE FEES RECEIVED BY DATALOOP FROM THE CUSTOMER IN RESPECT OF THE SIX (6) MONTHS IMMEDIATELY PRECEDING THE APPLICABLE CLAIM OR CAUSE OF ACTION.

10. Term and Termination

10.1. This Agreement will be in effect as of the Effective Date and shall continue in full force and effect for the Initial Term and shall renew automatically for successive Renewal Terms, as specified on the Order Form (the Initial Term, together with any Renewal Term(s), the "**Term**") unless either party provides a written notice to the other party of its wish not to renew no less than forty five (45) days prior to the end

of the then current term.

- 10.2. Notwithstanding the above, (i) in the case of breach by either party, the other party may terminate this agreement at any time by providing seven (7) days prior written notice to the breaching party (or without notice in the case of nonpayment); (ii) either party may terminate this Agreement with immediate effect upon written notice, in the event the other party: (i) makes a general assignment for the benefit of its creditors; (ii) applies for, consents to, or acquiesces to the appointment of a receiver, trustee, custodian, or liquidator for its business or assets; (iii) files, or consents to or acquiesces in, a petition seeking relief or reorganization under any bankruptcy or insolvency laws .
- 10.3. In the event of any termination for whatever reason, Customer shall have no further access to the Platform. Dataloop will make all Customer Materials available to Customer within 60 days as of the date of termination notice, following such period Customer Materials may not be available to Customer and may be deleted by Dataloop.
- 10.4. Sections 2-10 and 12 shall survive the expiration or termination of this Agreement for any reason.
11. **Publicity.** During the Term, Dataloop may refer to Customer as a customer of Dataloop, including by displaying Customer's name and logo on Dataloop's website and other marketing materials.
12. **General.** This Agreement sets forth the entire agreement between the parties regarding the subject matter hereof and supersedes all other agreements or understandings between the parties regarding such matters. No amendments or waivers shall be effective unless in writing and executed by both parties. Dataloop may assign all of its rights and obligations under this Agreement to a purchaser of all or substantially all of Dataloop's assets or share capital. Customer may not assign any rights or obligations under this Agreement to any third party and assignments in violation of the foregoing shall be void. Nothing in this Agreement creates any agency, employment, joint venture, or partnership relationship between the parties. This Agreement shall be governed by the laws of the State of Israel without regard to conflicts of law provisions thereof. The parties agree that the competent courts in Tel-Aviv, Israel shall have exclusive jurisdiction regarding all disputes hereunder, and the parties expressly consent to such jurisdiction. If any part of this Agreement is found invalid or unenforceable by a court of competent jurisdiction, such part shall be interpreted to give maximum effect to its terms as possible under applicable law, and the remainder of this Agreement shall remain in effect.

Schedule A Data Processing Agreement

This Data Processing Agreement ("**DPA**") forms an integral part of, and is subject to the Master Services Agreement, entered into by and between the Customer (as identified therein) ("**Controller**") and Dataloop Ltd. ("**Processor**", and the "**Agreement**", respectively). Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

Whereas, in connection with the performance of its obligations under the Agreement, Processor may Process Controller Personal Data (both as defined below) on behalf of the Controller; and

Whereas, the parties wish to set forth the mutual obligations with respect to the processing of Controller Personal Data by the Processor;

Now therefore, intending to be legally bound, the parties hereby agree as follows:

1. **Definitions.** In addition to capitalized terms defined elsewhere in this DPA, the following terms shall have the meanings set forth below:
 - 1.1. "**Applicable Law**" means Regulation 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) ("**GDPR**"), laws implementing or supplementing the GDPR.
 - 1.2. "**Controller Personal Data**" means any Personal Data Processed by Processor on behalf of Controller pursuant to or in connection with the Agreement.
 - 1.3. "**Data Protection Laws**" means Applicable Law and, to the extent applicable, the data protection or privacy laws of any other applicable country where the Services are provided or as agreed in writing between the Parties.
 - 1.4. "**Sub Processor**" means any person (excluding an employee of Processor) appointed by or on behalf of Processor to Process Controller Personal Data on behalf of the Controller in connection with the Agreement.
 - 1.5. The terms "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the meanings ascribed to them in the GDPR.
2. **Processing of Controller Personal Data.**
 - 2.1. Processor shall Process Controller Personal Data on Controller's behalf and at Controller's instructions as specified in the Agreement and in this DPA, including without limitation with regard to transfers of Controller Personal Data to a third country or international organization. Any other Processing shall be permitted only in the event that such Processing is required by any Data Protection Laws to which the Processor is subject. In such event, Processor shall, unless prohibited by such Data Protection Laws on important grounds of public

interest, inform Controller of that requirement before engaging in such Processing.

- 2.1.1. Controller instructs Processor (and authorizes Processor to instruct each Sub Processor) (i) to Process Controller Personal Data for the provision of the services, as detailed in the Agreement ("**Services**") and as otherwise set forth in the Agreement and in this DPA, and/or as otherwise directed by Controller; and (ii) to transfer Controller Personal Data to any country or territory as reasonably necessary for the provision of the Services and in accordance with Applicable Law.
 - 2.2. Controller sets forth the details of the Processing of Controller Personal Data, as required by Article 28(3) of the GDPR in **Appendix 1** (*Details of Processing of Controller Personal Data*), attached hereto.
3. **Controller.** Controller represents and warrants that it has and shall maintain throughout the term of the Agreement and this DPA, all necessary rights to provide the Controller Personal Data to Processor for the Processing to be performed in relation to the Services and in accordance with the Agreement and this DPA. To the extent required by Data Protection Laws, Controller is responsible for obtaining any necessary Data Subject consents to the Processing, and for ensuring that a record of such consents is maintained throughout the term of the Agreement and this DPA and/or as otherwise required under Data Protection Laws.
4. **Processor Employees.** Processor shall take reasonable steps to ensure that access to the Controller Personal Data is limited on a need to know and/or access basis and that all Processor employees receiving such access are subject to confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access to and use of Controller Personal Data.
5. **Security.** Processor shall implement appropriate technical and organizational measures to ensure an appropriate level of security of the Controller Personal Data including, as appropriate and applicable, the measures referred to in Article 32(1) of the GDPR. In assessing the appropriate level of security, Processor shall take into account the risks that are presented by the nature of the Processing and the information available to the Processor.
6. **Personal Data Breach.**
 - 6.1. Processor shall notify Controller without undue delay and, where feasible, not later than within 48 (forty eight) hours upon Processor becoming aware of a Personal Data Breach affecting Controller Personal Data. In such event, Processor shall provide Controller with reasonable and available information to assist Controller in meeting any obligations to inform Data Subjects or Supervisory Authorities of the Personal Data Breach as required under Applicable Law.
 - 6.2. At the written request of the Controller, Processor shall reasonably cooperate with Controller and take such commercially reasonable steps as are agreed by the parties or required under Applicable Law to assist in the investigation, mitigation and remediation of any Personal Data Breach.

7. **Sub Processing.**

- 7.1. Controller authorizes Processor to appoint (and permits each Sub Processor appointed in accordance with this Section 7 to appoint) Sub Processors in accordance with this Section 7.
- 7.2. Processor may continue to use those Sub Processors already engaged by Processor as identified to Controller as of the date of this DPA.
- 7.3. Processor may appoint new Sub Processors and shall give notice of any such appointment to Controller. If, within seven (7) days of such notice, Controller notifies Processor in writing of any reasonable objections to the proposed appointment, Processor shall not appoint the proposed Sub Processor for the Processing of Controller Personal Data until reasonable steps have been taken to address the objections raised by Controller and Controller has been provided with a reasonable written explanation of the steps taken. Where such steps are not sufficient to relieve Controller's reasonable objections, each of Controller or Processor may, by written notice to the other party and with immediate effect, terminate the Agreement to the extent that it relates to the Services requiring the use of the proposed Sub Processor. In such event, the terminating party shall not bear any liability for such termination.
- 7.4. With respect to each new Sub Processor, Processor shall:
 - 7.4.1. Prior to the Processing of Controller Personal Data by Sub Processor, take reasonable steps (for instance by way of reviewing privacy policies as appropriate) to ensure that Sub Processor is committed and able to provide the level of protection for Controller Personal Data required by this DPA; and
 - 7.4.2. ensure that the arrangement between the Processor and the Sub Processor is governed by a written contract, including terms that offer a materially similar level of protection for Controller Personal Data as those set out in this DPA and meet the requirements of Applicable Law.
- 7.5. Processor shall remain fully liable to the Controller for the performance of any Sub Processor's obligations.

8. **Data Subject Rights.**

- 8.1. Controller shall be solely responsible for compliance with any statutory obligations concerning requests to exercise Data Subject rights under Data Protection Laws (e.g., for access, rectification, deletion of Controller Personal Data, etc.). Processor shall, at Controller's sole expense, use commercially reasonable efforts to assist Controller in fulfilling Controller's obligations with respect to such Data Subject requests, as required under Data Protection Laws.
- 8.2. Upon receipt of a request from a Data Subject under any Data Protection Laws in respect to Controller Personal Data, Processor shall promptly notify Controller of such request and shall not respond to such request except on the

documented instructions of Controller or as required by Data Protection Laws to which the Processor is subject, in which case Processor shall, to the extent permitted by Data Protection Laws, inform Controller of such legal requirement prior to responding to the request.

9. **Data Protection Impact Assessment and Prior Consultation.** At Controller's written request and expense, the Processor and each Sub Processor shall provide reasonable assistance to Controller with respect to any Controller Personal Data Processed by Processor and/or a Sub Processor, with any data protection impact assessments or prior consultations with Supervisory Authorities or other competent data privacy authorities, as required under any Data Protection Laws.
10. **Deletion or Return of Controller Personal Data.** Processor shall promptly and in any event within 60 (sixty) days of the date of cessation of provision of the Services to Controller involving the Processing of Controller Personal Data, delete, return, or anonymize all copies of such Controller Personal Data, provided however that Processor may retain Controller Personal Data, as permitted by Applicable Law.
11. **Audit Rights.**
 - 11.1. Subject to Sections 11.2 and 11.3, Processor shall make available to an auditor mandated by Controller in coordination with Processor, upon prior written request, such information reasonably necessary to demonstrate compliance with this DPA and shall allow for audits, including inspections, by such reputable auditor mandated by the Controller in relation to the Processing of the Controller Personal Data by the Processor, provided that such third-party auditor shall be subject to confidentiality obligations.
 - 11.2. Any audit or inspection shall be at Controller's sole expense, and subject to Processor's obligations to third parties, including with respect to confidentiality.
 - 11.3. Controller and any auditor on its behalf shall use best efforts to minimize or avoid causing any damage, injury or disruption to the Processors' premises, equipment, employees and business. Controller and Processor shall mutually agree upon the scope, timing and duration of the audit or inspection and the reimbursement rate, for which Controller shall be responsible. Processor need not give access to its premises for the purposes of such an audit or inspection:
 - 11.3.1. to any individual unless he or she produces reasonable evidence of identity and authority;
 - 11.3.2. if Processor was not given a prior written notice of such audit or inspection;
 - 11.3.3. outside of normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis; or
 - 11.3.4. for the purposes of more than one (1) audit or inspection in any calendar year, except for any additional audits or inspections which:

11.3.4.1. Controller reasonably considers necessary because of genuine concern as to Processor's compliance with this DPA; or

11.3.4.2. Controller is required to carry out by Applicable Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Applicable Law in any country or territory, where Controller has identified its concerns or the relevant requirement or request in its prior written notice to Processor of the audit or inspection.

11.3.5. Processor shall immediately inform Controller if, in its opinion, an instruction received under this DPA infringes the GDPR or other applicable Data Protection Laws.

12. **Indemnity.** Controller shall indemnify and hold Processor harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Processor and arising directly or indirectly out of or in connection with a breach of this DPA and/or the Data Protection Laws by Controller.

13. **General Terms.**

13.1. **Governing Law and Jurisdiction.**

13.1.1. The parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

13.1.2. This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

13.2. **Order of Precedence.**

13.2.1. Nothing in this DPA reduces Processor's obligations under the Agreement in relation to the protection of Controller Personal Data or permits Processor to Process (or permit the Processing of) Controller Personal Data in a manner that is prohibited by the Agreement.

13.2.2. This DPA is not intended to, and does not in any way limit or derogate from Controller's obligations and liabilities towards the Processor under the Agreement and/or pursuant to Data Protection Laws or any law applicable to Controller in connection with the collection, handling and use of Controller Personal Data by Controller or other processors or their sub processors, including with respect to the transfer or provision of Controller Personal Data to Processor and/or providing Processor with access thereto.

13.2.3. Subject to this Section 13.2, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA

and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

13.3. Changes in Data Protection Laws.

13.3.1. Controller may, by at least 45 (forty five) calendar days' prior written notice to Processor, request in writing any variations to this DPA if they are required as a result of any change in, or decision of a competent authority under any Data Protection Laws in order to allow Controller Personal Data to be Processed (or continue to be Processed) without breach of that Data Protection Laws.

13.3.2. If Controller gives notice with respect to its request to modify this DPA under Section 13.3.1, (i) Processor shall make commercially reasonable efforts to accommodate such modification request and (ii) Controller shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Processor to protect the Processor against additional risks, or to indemnify and compensate Processor for any further steps and costs associated with the variations made herein.

13.3.2 **Severance.** Should any provision of this DPA be held invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Appendix 1: Details of Processing of Controller Personal Data

This **Appendix 1** includes certain details of the Processing of Controller Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Controller Personal Data.

The subject matter and duration of the Processing of the Controller Personal Data are set out in the Agreement, in Processor's Privacy Notice ("**Privacy Notice**") and this DPA.

The nature and purpose of the Processing of Controller Personal Data:

Rendering data management, data annotation and/or turn-key data labeling services as detailed in the Agreement and the Privacy Notice.

The types of Controller Personal Data to be Processed are as follows:

Personal Data included in images or video provided to Processor as Customer Materials (as defined in the Agreement).

The categories of Data Subject to whom the Controller Personal Data relates to are as follows:

Any individuals who are identified or identifiable in the Customer Materials provided by the Controller.

The obligations and rights of Controller.

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