Ziva Face Trainer
Data Processing Addendum

Updated: June 6, 2022

This Data Processing Addendum (this "**DPA**") is incorporated into and forms an integral part of the Ziva Face Trainer Terms of Service, or, as applicable, an offline agreement relating to the subject matter therein (the "**Terms of Service**") between Unity Technologies Canada Company, on behalf of itself and its Affiliates (collectively, "**Unity**") and you. Unity and Customer are herein each referred to as a "party" and collectively the "parties". Capitalized but undefined terms used in this DPA will have the meanings assigned to those terms in the Terms of Service.

Absent any other offline agreement between you and Unity, acceptance of the Terms of Service includes acceptance of this DPA.

1. Scope of Addendum

1.1. Applicable Data Protection Law. The parties agree that this DPA is designed to set forth the parties' obligations resulting from Applicable Data Protection Law. As such, the parties acknowledge and agree that this DPA will only apply to the extent, as applicable, that (a) EU Data Protection Law applies to the processing of personal data of data subjects located in or from Customer located (or where Customer is a processor, where the relevant controller is located) in the EEA, UK, or Switzerland, (b) the LGPD applies to the processing of personal data of data subjects located in Brazil and to any processing activity that is for the purpose of providing goods or services in Brazil, (c) the PIPEDA applies to the processing of personal data of data subjects located in Canada; (d) Personal Data Protection Act, Act No. 25.326 of 2000 applies to the processing of personal data within the territory of Argentina, and (e) the CCPA applies to the processing of personal data of data subjects located in the State of California, United States of America.

1.2. Other Data Protection Law. Notwithstanding the foregoing, where applicable, certain Additional Terms for Other Data Protection Law will supplement this DPA, as set forth Section 6.

The parties acknowledge and agree that this DPA will only apply to the extent that Customer is a data subject or the transaction between Customer and Unity as described in the Terms of Service are regulated under Applicable Data Protection Laws or other data protection laws referenced herein.

2. Definitions

2.1. "controller", "processor", "data subject", "personal data", "personal data breach", "processing", and "process" shall have the meanings given in EU Data Protection Law where such law applies; and (ii) where CCPA applies, the definition of "personal data" includes "Personal Information", the definition of "data subject" includes "Consumer", the definition of "controller" includes "Business", and the definition of "processor" includes "Service Provider".

2.2. “**Additional Terms for Other Data Protection Laws**” means the additional terms referred to in Section 6, which reflect the parties’ agreement on the terms governing the processing of certain data in connection with certain other data protection regulations not covered in Sections 3 and 4 .

2.3. “**Affiliates**” means an entity that directly or indirectly controls, is controlled by, or is under common control with, a party.

2.4. “**Applicable Data Protection Law**” means EU Data Protection Laws, the California Consumer Privacy Act (“**CCPA**”); the Canadian Personal Information Protection and Electronic Documents Act (“**PIPEDA**”); the Brazilian General Data Protection Law ("**LGPD**"); and Argentina Data Protection Law.

2.5. “**Argentina Data Protection Law**” means Personal Data Protection Act, Act No. 25.326 of 2000 ('the Act') and Decree No.1558/2001 Regulating Law No. 25.326 ('the Decree'), amended by DecreeNo. 1160/10.

2.6. “**Argentinian Model Clauses**” mean the model contract for the international transfer of “personal data” (as defined under Argentina Data Protection Law) to other countries that do not provide an adequate level of protection for personal data related to Data Subjects residing in Argentina, as set out in Disposition 60-E/2016.”

2.7. “**Customer**” or “**You**” means either an individual utilizing any of the Services in his or her individual capacity or the Legal Entity affiliated with an individual utilizing the Services on behalf of such Legal Entity.

2.8. “**End User**” means Customer and/or the viewers of Customer content, including content created through use of the Services as detailed in the Terms of Service.

2.9. "**EU Data Protection Law**" means (i) the EU General Data Protection Regulation 2016/679; (ii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iii) any national data protection laws made under or pursuant to (i) or (ii).

2.10. “**Legal Entity**” means a company, organization or other legal entity.

2.11. “**Services**” means the Services used by Customer pursuant to the Terms of Service.

2.12. “**Sub-Processor**” means any entity that Unity engages to process Customer’s personal data on behalf of Unity, which entities may include Unity’s Affiliates.

3. General Terms and Conditions

3.1. Control/Application of this DPA. In the event of any conflict or discrepancy between the Additional Terms for Other Data Protection Laws, the Terms of Service, and this DPA, the following order of precedence will apply: (a) the Additional Terms for Other Data Protection Laws, (b) this DPA,

and (c) the Terms of Service. This DPA applies only to Customer, and Unity and does not confer any rights to any third party hereunder. This DPA does not replace any additional rights related to privacy or data security set forth in the Terms of Service and does not enlarge any rights provided for in the Terms of Service. Customer continues to be limited to the data use rights and restrictions provided for in the Terms of Service.

3.2. Limitations of Liability. This DPA in no way alters the limitations of liability or other legal terms set out in the Terms of Service.

3.3. Compliance with Law/Public Notices. Each party will maintain a publicly-accessible privacy policy on its website that satisfies the transparency disclosure requirements of Applicable Data Protection Law. Customer will list Unity as a third party that is collecting data within its application in its publicly available privacy policy, including by providing a link to Unity's privacy policy. Customer agrees to keep updated versions of Unity software and services installed in their applications as Unity identifies necessary to permit Unity to maintain its compliance with law.

3.4. Term and Termination. This DPA becomes effective as of the date that Customer accepts the Terms of Service and terminates simultaneously and automatically upon the termination or expiration of the Terms of Service. Unity may terminate this DPA (in whole or in part) at any time upon notice to Customer if Unity offers alternative means to Customer that complies with Applicable Data Protection Laws. Customer may terminate this DPA at Customer's discretion upon Unity's receipt of Customer's written notice of termination. Customer acknowledges that termination of this DPA may prevent Customer from being able to further utilize the Services in absence of other agreement with Unity in respect of compliance with Applicable Data Protection Law.

3.5. Governing Law. To the extent required by Applicable Data Protection Law, this DPA will be governed by the laws of the applicable jurisdiction. In all other cases, this DPA will be governed by the laws of the jurisdiction set forth in the Terms of Service.

3.6. Survival. This DPA shall survive termination or expiry of any terms of service or other agreement to permit Unity to comply with its legal obligations. Upon termination or expiry of the Parties' relationship, Unity may continue to process the personal data provided that such processing complies with the requirements of this Section 3.6 and otherwise with Applicable Data Protection Law.

4. Processing of Personal Data

4.1. Relationship of the Parties**.** The parties acknowledge and agree that with regard to the processing of personal data for the Services: (a) Customer is a controller or processor, as applicable, of the personal data under Applicable Data Protection Law; (b) Unity is a processor of the personal data under Applicable Data Protection Law or, where Customer is a processor, Unity is a sub-processor of the personal data under Applicable Data Protection Law; and (c) each party will comply with the obligations applicable to it under Applicable Data Protection Law with respect to the processing of

personal data. If Customer is a processor, Customer represents and warrants to Unity that Customer's instructions and actions with respect to personal data, including its appointment of Unity as another processor, have been authorized by the relevant controller.

4.2. Customer's Instructions. For the purposes of this DPA, Customer instructs Unity to process personal data for the following purposes: (i) to store and use data as described in the Terms of Service and any applicable descriptions of the Services, including for the maintenance and improvement of the Services; and (ii) to comply with other reasonable instructions provided by Customer where such instructions are consistent with the Terms of Service, this DPA, and Applicable Data Protection Law (collectively, the "the "***Permitted Purpose***"). This DPA and the Terms of Service constitute Customer's complete and final instructions to Unity for the Processing of Customer personal data. Any additional instructions that are inconsistent with the terms of the Terms of Service or this DPA must be agreed in writing signed by authorized representatives of both parties.

4.3. Unity's Processing of Personal Data. In connection with Customer's use of the Services, Unity will only process personal data on behalf of and in accordance with Customer's instructions, which includes instruction to maintain and improve the Services, and otherwise in accordance with the requirements of Applicable Data Protection Law. Customer's instructions for the Processing of personal data by Unity will comply with all Applicable Data Protection Law. Customer will have sole responsibility for the accuracy, quality, and legality of the personal data and the means by which Customer acquired such personal data. Customer agrees that Unity may and instructs Unity to transfer data to sub-processors in third countries under adequate protections equal to those found herein.

4.4. Security of Processing; Responding Personnel. Unity will secure Customer's personal data by implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as required under Applicable Data Protection Law. Unity will not materially decrease the overall security of the Services during the term of the Terms of Service. Certain of Unity's employees have been appointed as data protection officers where such appointment is required by Applicable Data Protection Law. The appointed person may be reached at dpo@unity3d.com.

4.5. Personal Data Breach Notification. Unity will notify Customer without undue delay after it becomes aware of a personal data breach. To the extent such personal data breach is caused by a violation of the requirements of this DPA by Unity, Unity will make reasonable efforts to identify and remediate the cause of such personal data breach. Any notification of a personal data breach provided hereunder will not be construed as an acknowledgement by Unity of any fault or liability in connection with the personal data breach. Further, Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any personal data breach.

4.6. Compliance Assistance. Upon request from Customer, Unity will provide commercially reasonable assistance to Customer by appropriate technical and organizational measures, insofar as this is possible, for handling of a Data Subject's requests and assistance in Customer's compliance with

the EU Data Protection Laws. Any such assistance will take into account the nature of Unity's processing of personal data and the information available to Unity, and will be provided solely to the extent that Customer is unable to fulfill such requests through the Services and at Customer's cost.

4.7. Data Subject Requests. Notwithstanding the foregoing, if Unity receives a request from a data subject in relation to personal data, Unity will direct the data subject to submit his or her data subject request to Customer, and Customer will be responsible for responding to such request.

4.8. Government Requests. Unity will notify Customer about any legally binding request for disclosure of the personal data by a law enforcement or other public authority unless otherwise prohibited.

4.9. Deletion of Customer Personal Data. Unity will delete all personal data and copies thereof, excluding backup systems, upon the request of Customer following termination or expiration of the Terms of Service and otherwise will only otherwise hold data for as long as there is a business need. Customer is required to set a retention period by Applicable Data Protection Law and will effectuate such retention period by deleting its own data from Unity systems on a self service basis. Further, Unity will effectuate a backstop retention period by setting a concomitant rolling deletion cycle, with Customer's data being subject to automatic deletion as a matter of course. The parties agree that the certification of the deletion of Customer personal data will be provided by Unity to Customer upon Customer's request.

4.10. Audits. Unity will make available to you all information necessary to demonstrate compliance with its obligations under the GDPR or UK GDPR. Upon your written request at reasonable intervals, Unity will provide a copy of Unity's then most recent summaries of third-party audits or certifications or other documentation, as applicable, that Unity generally makes available to its Customers at the time of such request.

4.11. Unity Personnel.

4.11.1. Confidentiality. Unity will ensure that its personnel engaged in the processing of personal data are informed of the confidential nature of personal data, have received appropriate training on their responsibilities, and have either executed written confidentiality agreements no less protective than the confidentiality provisions set forth in Terms of Services or are under an appropriate statutory obligation of confidentiality. Unity will ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.11.2. Limitation of Access. Unity will ensure that Unity's access to personal data is limited to those personnel who require such access to perform under the Terms of Service.

4.11.3. Data Protection Officer. Certain of Unity's employees have been appointed as data protection officers where such appointment is required by Applicable Data Protection Law. The appointed person may be reached at dpo@unity3d.com.

4.12. Sub-Processors.

4.12.1. General Authorization. To the extent required by Applicable Data Protection Law, Customer authorizes Unity to subcontract processing of personal data under this DPA to Sub-processors, provided that Unity: (a) provides Customer with information about the Sub-processor(s) as may be reasonably requested by Customer from time to time; (b) flows down its obligations under this DPA to such Sub-processor, such that the processing requirements of such Sub-Processor with respect to Customer's personal data are no less onerous than the processing requirements of Unity as set forth in this DPA; and (c) will be fully liable to Customer for the performance of the Sub-Processor's obligations under this DPA if such Sub-Processor fails to fulfill its data protection obligations.

4.12.2. New Sub-Processors. Unity will inform Customer of any intended changes concerning the addition or replacement of Sub-processors and provide Customer with five (5) business days to make reasonable objections to any new Sub-processors. In the event Customer reasonably objects to a new Sub-processor, you may, as a sole remedy, terminate the Terms of Service and this DPA with respect only to those Services that cannot be provided by Unity without the use of the objected-to Sub-processor by providing Unity with written notice provided that all amounts due under the Terms of Service shall be duly paid to Unity.

5. Changes to this DPA.

Unity may update the terms of this Addendum from time to time, including, but not limited to: (a) as set forth herein; (b) as required to comply with Applicable Data Protection Law, applicable regulation, court order, or regulatory guidance; or (c) to add new Additional Terms for Other Data Protection Laws. If such an update will have a material adverse impact on Customer, as reasonably determined by Unity, then Unity will use reasonable efforts to inform Customer at least 30 days (or such shorter period as may be required to comply with Applicable Data Protection Law) before the change will take effect. If Customer objects to any such change, Customer may terminate this DPA by giving written notice to Unity within 30 days of being informed by Unity of the change. Customer acknowledges that termination of this DPA may prevent Customer from being able to further utilize the Services in absence of other agreement with Unity in respect of compliance with Applicable Data Protection Law.

6. Additional Terms for Other Data Protection Laws

The parties acknowledge that data protection laws in addition to Applicable Data Protection Law may apply to the parties' processing of Personal Data. Terms and conditions related to such other data protection laws are addressed in this Section 6.

6.1. Japan & Japanese Data Protection Laws. This Section applies to all transfers and provisions of Personal Information or Personal Data from Customer to Unity as contemplated by the Terms of Service if the Personal Information or Personal Data is regulated under the Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2015 and thereafter) (**'APPI'**), including where applicable, rules, guidance and codes of practices issued by the regulatory bodies of Japan hereinafter,

"**Japanese Data Protection Laws**." Any term not otherwise defined in this DPA shall have the meaning ascribed to it by the Japanese Data Protection Laws.

6.1.1. To the extent that the Services are subject to Japanese Data Protection Laws the definition of "processor" includes an entity entrusted by the Business Operator Handling Personal Information the handling of Personal Information or Personal Data in whole or in part within the scope necessary for the achievement of the purpose of utilization (also a "trustee"), as described under Japanese Data Protection Laws. Customer may exercise necessary and appropriate supervision over the trustees including subcontractors to ensure the proper security management of the Personal Information or Personal Data.

6.1.2. Customer is responsible for providing any consents and notices required to permit (a) Customer's use and receipt of the Services and (b) Unity accessing, storing, and processing of data provided by Customer (including Personal Information or Personal Data, if applicable) under the DPA. Additionally, Customer agrees to obtain the consent of each principal to the Provision of Personal Data to a Third Party including those in a Foreign Country as contemplated under this DPA by providing necessary information for the principal to give consent thereto, if and to the extent required under the Japanese Data Protection Laws.

6.1.3. Customer is responsible for providing any consents and notices required to permit Unity accessing, storing, and processing of data provided by Customer (including Personal Information or Personal Data, if applicable) under the DPA. Additionally, Customer agrees to obtain the consent of each principal to the Provision of Personal Data to a Third Party including those in a Foreign Country as contemplated under this DPA providing necessary information for the principal to give consent thereto, if and to the extent required under the Japanese Data Protection Laws.

6.1.4. Purpose of Use.The Customer shall permit Unity to utilize the Personal Information or Personal Data within the scope of the Permitted Purpose.

6.1.5. Compliance. Unity and the Customer shall warrant that the necessary proceedings under the Japanese Data Protection Laws have been implemented, including, without limitation, the recording of any transfer of Personal Data to a Third Party or receipt of Personal Data from a Third Party.

6.1.6. Safety Measures. Unity and the Customer shall comply with Japanese Data Protection Laws and take necessary measures for the management of Personal Information or Personal Data.

6.1.7. In the case that the Customer provides Personal Information or Anonymously Processed Information, or Pseudonymously Processed Information under Japanese Data Protection Laws to Unity in effecting the Permitted Purpose, the Customer shall specify to that effect in advance. In the case that the Customer provides Anonymously Processed Information or Pseudonymously Processed Information to Unity in effecting the Permitted Purpose, the

Customer shall warrant that the proceedings under the Japanese Data Protection Laws have been implemented with respect to the Anonymously Processed Information or Pseudonymously Processed Information in order to qualify as such.

6.1.8. Unity shall, if the data have been provided in accordance with this Section, comply with Japanese Data Protection Laws and take any measures required thereof for the management of the applicable data.

6.1.9. Unity shall at all times implement appropriate technical, physical, personnel and organizational measures designed to safeguard Personal Information or Personal Data as required by Japanese Data Protection Laws.

6.2. South Korea & Korean Data Protection Laws. This Section applies to all transfers and provisions of Personal Information from Customer to Unity as contemplated by the Terms of Service if the personal information is within the scope of the Personal Information from Customer and Unity from South Korea as contemplated by the Terms of Service. Terms not otherwise defined in this DPA shall have the meaning ascribed to it by the Personal Information Protection Act, the Enforcement Decree and the Enforcement Rule thereof, the Standards on Measures to Ensure Personal Information Security (Personal Information Protection Commission Notification No. 2020-2), the Standard Guidelines on Protection of Personal Information Personal Information Protection Commission Notification No. 2020-1), including where applicable rules, guidances and codes of practices issued by the regulatory bodies of South Korea. Hereinafter referred to "**Korean Data Protection Laws.**"

6.2.1. To the extent the Services are subject to Korean Data Protection Laws the Customer hereby entrusts Unity as a Service Provider and Unity hereby agrees to provide the processing of personal information related to the Permitted Purposes.

6.2.2. Service Provider shall perform personal information processing for the Services in accordance with the terms and conditions of this DPA.

6.2.3. Unless otherwise approved by the Customer in advance, Service Provider may not transfer or re-entrust all or a part of its rights and obligations hereunder to a third party. If Service Provider enters into an entrustment agreement with a third party in connection with this DPA, Service Provider shall inform and consult with the Customer prior to the execution of entrustment agreement.

6.2.4. Service Provider shall take managerial and technical measures necessary for securing safety of the personal information pursuant to Articles 23(2), 24(3) and 29 of the Personal Information Protection Act, Articles 21 and 30 of the Enforcement Decree thereof and the Standards on Measures to Ensure Personal Information Security (Personal Information Protection Commission Notification No. 2020-2).

6.2.5. Service Provider shall not use the personal information beyond the scope of the tasks entrusted hereunder or disclose or divulge the personal information to any third party during the term of this DPAas well as after the termination of this DPA. Upon the termination or expiration of this DPA, Service Provider shall destroy or promptly return to the Customer the personal information in its possession regarding the tasks entrusted hereunder pursuant to Article 16 of the Enforcement Decree of the Personal Information Protection Act and the Standards on Measures to Ensure Personal Information Security (Personal Information Protection Commission Notification No. 2020-2). If Service Provider destroys the personal information in accordance with the above, Service Provider shall give notice thereof the Customer without undue delay.

6.2.6. The Customer may supervise Service Provider in connection with the following matters, and Service Provider shall reasonably comply with such supervision: (i) status of the personal information processing; (ii) status of those who can access the personal information and access logs thereof; (iii) compliance of the provisions prohibiting use or third party transfer of the personal information outside the scope of the intended purpose or re-entrustment; (iv) enforcement of measures necessary for securing safety such as encryption, etc.; and (v) other matters necessary for the protection of personal information.

6.2.7. The Customer may reasonably request documentation to inspect the status of the matters set forth in the section above and require the Service Provider to make necessary corrections thereto. Service Provider shall make commercially reasonable efforts to comply with such requests and make such corrections unless it has a justifiable reason.

6.2.8. The Customer reserves the right to conduct training for Service Provider once a year in order to prevent loss, theft, leakage, alteration or damage of personal information, and Service Provider agrees to attend such training by the Customer. The details of the training, including the time and method, shall be implemented upon consultation between the Customer and Service Provider as necessary.

6.2.9. Either party shall indemnify the other party, data subject or any third party for any damages due to the breach of this Section 6.2 by itself or its officer, employee or trustee, or any damages due to termination of this DPA for causes attributable to itself or its officer, employee or trustee. if the other party compensates for all or a part of the damage incurred by the data subject or other third party, the other party has the right to claim reimbursement from the offending party.

6.3. Singapore & Singapore Data Protection Laws. This Section applies to all transfers and disclosures of Personal Data from Customer to Unity as contemplated by the Terms of Service if the personal data is within the scope of the Singapore's Personal Data Protection Act 2012 (No. 26 of 2012), including where applicable, rules, guidance and codes of practices issued by the regulatory bodies of Singapore

hereinafter, "**Singapore Data Protection Laws**". Terms not otherwise defined in this DPA shall have the meaning ascribed to it by the Singapore Data Protection Laws

6.3.1. To the extent that the Services are subject to Singapore Data Protection Laws the definition of "processor" includes a "data intermediary" as described under Singapore Data Protection Laws. Customer may exercise necessary and appropriate supervision over the data intermediary to ensure proper security management of the personal data

6.3.2. Customer is responsible for any consents and notices required to permit (a) Customer's use and receipt of the Processor's Services and (b) Unity accessing, storing, and processing of data provided by Customer (including Personal Information, if applicable) under the Terms of Service and this DPA. Additionally, Customer agrees to obtain the consent of each Data Subject to an International Transfer as contemplated under this DPA if and to the extent required under the Singapore Data Protection Laws. Personal Information may be transferred, as necessary, world-wide to provide the Processor Services under the Terms of Service and this DPA.

6.3.3. Purpose. Unity shall comply with all its obligations under the PDPA at its own cost. Unity shall only process, use, or disclose Customer Personal Data: strictly for the within the scope of the Permitted Purpose to fulfill its obligations and provide the Services re; with the Customer's prior written consent; or when required by law or and order of court, but shall notify the Customer as soon as practicable before complying with such law or order of court at its own costs.

6.3.4. Accuracy and Correction of Personal Data. Where the Customer provides Customer Personal Data to Unity, the Customer shall make reasonable effort to ensure that the Customer Personal Data is accurate and complete before providing the same to Unity. Unity shall put in place adequate measures to ensure that the Customer Personal Data in its possession or control remains or is otherwise accurate and complete. In any case, Unity shall take steps to correct any errors in the Customer Personal Data, as soon as practicable upon the Customer's written request.

6.3.5. Protection. Unity shall protect Customer Personal Data in Unity's control or possession by making reasonable security arrangements (including, where appropriate, physical, administrative, procedural and information & communications technology measures) to prevent unauthorized or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of Customer Personal Data, or other similar risks.

6.3.6. Retention limitation. Unity shall not retain Customer Personal Data (or any documents or records containing Customer Personal Data, electronic or otherwise) for any period of time longer than is necessary to serve the purposes of this Terms of Service and this DPA.

6.3.7. Policies on personal data protection. Unity shall ensure that its employees, agents and subcontractors who may receive or have access to any of Customer Personal Data are aware of the obligations specified under this clause and agree to abide by the same.

6.3.8. Access. The Contractor shall provide the Customer with access to the Customer Personal Data that the Contractor has in its possession or control, as soon as practicable upon Customer's written request.

6.4. Illinois & BIPA. This Section applies to all transfers and disclosures of Personal Data from Customer to Unity as contemplated by the Terms of Service, particularly where such data consists of an individual voiceprint or any geometric scans of the facial features of an individual ("**Biometric Information**") and is within the scope of the Illinois Biometric Information Privacy Act, hereinafter "**BIPA**". Terms not otherwise defined in this DPA shall have the meaning ascribed to it by BIPA.

6.4.1. Customer must comply with BIPA, including but not limited to, providing proper notification of the transfer, communicating the possibility that an individual's data will be transmitted outside their country of origin, and obtaining any necessary consents for both collection and storage of biometric data.

6.4.2. Where Biometric Information is used by Customer and transmitted to Unity in connection with the Services, Customer will obtain advance, adequate consents from those persons whose Biometric Information has been used. Such consent will be substantially similar to the following: "in accepting these terms, the individual providing his/her biometric information gives his/her written consent to the Customer to collect, store, disclose and use his Biometric Information".

6.4.3. Unity shall secure Biometric Information in the same manner as any other confidential or sensitive information that it stores. The information shall be destroyed upon conclusion of its use as specified elsewhere in this DPA.