Unity – Data Processing Addendum

Effective : April 3, 2023

This Data Processing Addendum (this "DPA") is incorporated into and forms an integral part of the Unity Terms of Service, available at https://unity3d.com/legal/terms-of-service,the Unity Advertising Terms of Service, available at https://unity3d.com/legal/one-operate-services-terms-of-service, the Asset Store Terms of Service and EULA, available at https://unity.com/legal/as-terms, and the Asset Store Provider Agreement, available at https://unity.com/legal/as-provider, or, as applicable, an offline agreement relating to the subject matter therein (the "Terms of Service") between You and the Unity Party specified in Section 2.22 below., on behalf of itself and its Affiliates (collectively, "Unity") and you ("Customer" or "you"), each a "party" and collectively the "parties". Acceptance of the Terms of Service includes acceptance of this DPA. Capitalized but undefined terms used in this DPA will have the meanings assigned to those terms in the Terms of Service.

To the extent you are using the services named herein and absent any other offline agreement, you shall be deemed to have accepted this DPA and applicable Standard Contractual Clauses upon acceptance or execution of the applicable Terms of Service. This is a pre-signed copy of this document and accompanying SCCs which you may download, execute on your side, and return to DPA@unity3d.com.

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) the Private Sector Act applies to the processing of personal data of data subjects located in Québec; (e) Personal Data Protection Act, Act No. 25.326 of 2000 applies to the processing of personal data within the territory of Argentina, (f) the CCPA as amended applies to the processing of personal data of data subjects located in the State of California, United States of America, (g) the CPA applies to the processing of personal data of data subjects located in the State of Colorado, United States of America, (h) the VCDPA applies to the processing of personal data of data subjects located in the State of Virginia, United States of America, (i) the CTDPA applies to the processing of personal data of data subjects located in the State of Connecticut, United States of America, and (j) the UCPA applies to the processing of personal data of data subjects located in the State of Utah, United States of America.

1.2 Non-Applicable Data Protection Law. Notwithstanding the foregoing, where applicable, certain Additional Terms for Non-Applicable Data Protection Law will supplement this DPA, as set forth Section 8.

2. Definitions

2.1 "controller", "processor", "data subject", "personal data", “personal data breach”, "processing" (and "process"), and “special category” shall have the meanings given in EU Data Protection Law; provided, however, that:

2.1.1 To the extent that the CCPA is applicable, 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”, all as defined under the CCPA , and

2.1.2 To the extent that Non-EU Data Protection Law is applicable, definitions shall have the meanings given under applicable law.

2.2 “Additional Terms for Non-Applicable Data Protection Law” means the additional terms referred to in Section 8, which reflect the parties’ agreement on the terms governing the processing of certain data in connection with certain other data protection regulations.

2.3 “Advertiser” means any party placing advertisements with Unity pursuant to the Terms of Service.

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

2.5 “Applicable Data Protection Law” means (i) EU Data Protection Law; and (ii) Non-EU Data Protection Law.

2.6 “Approved Addendum” means the template addendum issued by the United Kingdom Information Commissioner’s Office and laid before the United Kingdom Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of such addendum.

2.7 “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 Decree No. 1160/10.

2.8 “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.”

2.9 “Biometric Laws” means any law or regulation governing the handling of biometric information, including but not limited to the Illinois Biometric Information Privacy Act (“BIPA”), and the Texas Capture or Use of Biometric Identifier Act (“CUBI”).

2.10 “Compliance Tool” means Unity’s self-serve tools made available to data subjects by Unity for the purposes of exercising their rights under Applicable Data Protection Law.

2.11 “DPA 2018” means the UK Data Protection Act, 2018.

2.12 “End User” means customers of Customer and/or the viewers of Publishers’ and/or Advertisers’ content

2.13 "EU Data Protection Law" means (i) the GDPR; (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) including the UK GDPR and the DPA 2018.

2.14 “GDPR” means the EU General Data Protection Regulation 2016/679.

2.15 “Non-EU Data Protection Law” means the California Consumer Privacy Act (“CCPA”), as amended by the California Privacy Rights Act (“CPRA”); the Virginia Consumer Data Protection Act (“VCDPA”); the Colorado Privacy Act (“CPA”), the Connecticut Data Protection Act (“CTDPA”), the Utah Consumer Privacy Act (“UCPA”); the Canadian Personal Information Protection and Electronic Documents Act (“PIPEDA”); Québec's Act Respecting the Protection of Personal Information in the Private Sector (“Private Sector Act”), the Brazilian General Data Protection Law ("LGPD"); and Argentina Data Protection Law.

2.16 “Publisher” means any distributor of software and services for whom Unity provides monetization or backend services for such publisher’s software and services under the Terms of Service.

2.17 “SCCs” means with respect to data transfers from the European Union to third countries that are not deemed adequate jurisdictions by the European Commission the Controller-Controller standard contractual clauses (the “C2C SCCs”) and/or Controller-Processor standard contractual clauses (the “C2P SCCs”) (as applicable) approved by the European Commission, as may be updated from time to time (the “EU SCCs”) or, with respect to data transfers from the United Kingdom, the C2C SCCs and/or the C2P SCCs as further amended by the Mandatory Clauses of the Approved Addendum, as may be updated by the United Kingdom Information Commissioner’s Office from time to time (the “UK SCCs”), for so long as this DPA is effective, subject to the following: (i) only the provisions pertaining to Module One are deemed applicable under the C2C SCCs standard contractual clauses; (ii) only the provisions pertaining to Module Two are deemed applicable under the C2P SCCs; (iii) except with respect to the UK SCCs, the governing law will be that of the country of the Data Protection Authority with jurisdiction over the data exporter and any dispute arising in connection with the EU SCCs will be subject to the exclusive jurisdiction of the courts of such country; (iv) the applicable annex to the applicable standard contractual clauses is amended as set forth in Appendix A below.

2.18 "Security, Privacy and Architecture Documentation" means the Security, Privacy and Architecture Documentation applicable to the Services purchased by Customer, as described in summaries that Unity generally makes available to its Customers as updated from time to time, or otherwise made reasonably available by Unity.

2.19 "Services" means the Controller Services and/or Processor Services (as outlined in Section 3) used by Customer in connection with the applicable Terms of Service.

2.20 "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.

2.21 "UK GDPR" means the EU General Data Protection Regulation 2016/679, as incorporated into UK Data Protection Law.

2.22 "Unity Party" means the entity responsible for the data processing activities.

2.22.1 Unless otherwise noted in this section 2.22, Unity Party for all Services governed by the **Unity Terms of Service** shall be Unity Technologies S.F.

3. Controller Services and Processor Services

3.1 Controller Services.

3.1.1 Unless otherwise noted in 3.2 , "Controller Services" shall refer to all Services governed by the applicable Unity Terms of Service.

3.2 Processor Services.

3.2.1 "Processor Services'' as used herein shall refer to

Game Services (including Engage Services)
Multiplayer Services (not including Safe Voice which is a Controller Service)
UGS and Advertising Consulting Services
Unity MARS and the Unity AR Companion App
PlasticSCM
Ziva Face Trainer
SyncSketch
Unity LevelPlay
Furioos

4. General Terms and Conditions

4.1 Control/Application of the DPA. In the event of any conflict or discrepancy between the SCCs, the Additional Terms for Non-Applicable Data Protection Law, the Terms of Service, and the terms and conditions of this DPA, the following order of precedence will apply: (a) the SCCs (where applicable), (b) the Additional Terms for Non-Applicable Data Protection Law, (c) this DPA, and (d) 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.

4.2 Treatment of Data Rights and Restrictions in Other Agreements. Customer agrees that this DPA does not enlarge any rights provided for in the Terms of Service, and Customer continues to be limited to the data use rights and restrictions provided for therein.

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

4.4 Advertiser's Mobile Measurement Partners. Where Customer is an Advertiser, it agrees that, to the extent it requires Unity to present data to a third party install tracker in connection with trafficking of its advertising campaigns, that it has such third parties under a valid data processing agreement clearly directing the install tracker as to its usage instructions, duties, and liabilities for processing such data.

4.5 Special Category Data. With the exception of biometric information uploaded through the use of Ziva Face Trainer, Unity MARS, Unity AR Companion App, and Safe Voice, Special Category Data will not be processed pursuant to this DPA and the Customer warrants and represents that the Customer will not be sharing, disclosing or otherwise transferring such data to Unity.

4.5.1 You represent and warrant that you have complied with all Data Protection Laws with respect to any transfer of Person Data to us in connection with your use of the Service. Such compliance by you includes, but is not limited to, you providing proper notification of the transfer, communicating the possibility that a person's data may be transmitted outside their country of origin, and obtaining any necessary consents for both collection and storage of biometric information of such person, including any geometric scans of that individual's facial features. Further, where applicable, you give your written consent to Unity to collect, store, disclose and use any biometric information contained in Your Materials from which Created Materials will be provided as part of the Service. Please note that Unity may request copies of your consent records to confirm your compliance with this Section 4.5.1. Failure to provide proper documentation may result in cancellation of your use of the Service.

4.5.2 Biometric Laws_ 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 applicable Biometric Laws including but not limited to BIPA and CUBI. Terms not otherwise defined in this DPA shall have the meaning ascribed to it by Applicable Data Protection Law

4.5.2.1 Customer must comply with Biometric Laws, 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.

4.5.2.2 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 in compliance with applicable Biometric Laws and Applicable Data Protection Law.

4.5.2.3 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.

4.6 Compliance with Law/Public Notices. Each party shall maintain a publicly-accessible privacy policy on its website that satisfies the transparency disclosure requirements of Applicable Data Protection Law. Customer shall 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. To the extent required by Applicable Data Protection Law, the Parties agree that they will specifically identify to the other Party when they require that the Party obtain from the relevant individuals their explicit consent pursuant to Applicable Data Protection Law, thereby permitting the use of his or her Personal Data by the receiving Party as contemplated by that Party. The foregoing does not create a general requirement related to Consent, and a Party requiring Consent must provide adequate notice to the other Party of this requirement. Customer agrees to keep up to date versions of Unity software and services installed in their applications as Unity identifies as necessary to permit Unity to maintain its compliance with law. By way of example and without limiting the generality of the foregoing, Unity relies on Customer updating its applications with software changes made to provide certain opportunities for End Users to exercise their rights to disclosure and deletion requests; however, updates unrelated to compliance with law may occur from time to time which are not subject to this Section 4.6 nor governed by this DPA.

4.7 Term and Termination. This DPA will become effective as of the date Customer has accepted both: (i) a valid Terms of Service; and (ii) solely to the extent this DPA is not already

incorporated into such Terms of Service, this DPA. Subject to Section 4.9, This DPA will terminate simultaneously and automatically upon the termination 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.

4.8 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 shall be governed by the laws of the jurisdiction set forth in the Terms of Service.

4.9 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 4.9 and otherwise with Applicable Data Protection Law.

5. Controller-Controller Terms. The Controller-Controller Terms set forth in this Section 5 will apply only in connection with Customer's use of the Controller Services and Unity's processing of personal data in connection therewith.

5.1 Relationship of the Parties. Subject to Section 4.2, the parties acknowledge and agree in connection with the processing of personal data for Controller Services, each party (a) is an independent controller of the personal data under Applicable Data Protection Law; (b) will individually determine the purposes and means of its processing of personal data; and (c) will comply with the obligations applicable to it under Applicable Data Protection Law with respect to the personal data.

5.2 Purpose of Processing. Customer will permit the disclosure of the personal data described in the Terms of Service or otherwise herein for the applicable Controller Services to Unity to process as a controller of the personal data for the purposes described in Unity's Privacy Policy as applicable by Controller Services to which Customer subscribes (the "Permitted Purpose"). Specifically, and notwithstanding anything to the contrary in any prior data processing addendum, Unity shall use the personal data in an identified format to make decisions (including targeting decisions) within its services, provide services (including monetization services) to its customers, assist its customers with maintaining their own services, improving its services, and analyzing the marketplace for its services as well as the performance of its services. Notwithstanding the foregoing, data obtained by Unity independent of Customer using Unity software or services that is the same or similar to the personal data described herein shall not be restricted by this Addendum, any license agreement, or any terms or conditions for such services. For the avoidance of doubt, Unity may use all personal data collected on an aggregated or de-identified basis as set out in its Privacy Policy, provided that such use does not reveal an individual or an individual's device directly or indirectly.

5.3 Security. Each party shall implement appropriate technical and organizational measures to protect the personal data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the personal data (a "Security Incident"). In the event that a party suffers a confirmed Security Incident, it shall notify the other party without undue delay and both parties shall cooperate in good faith to agree and action such measures as may be necessary to mitigate or remedy the effects of the Security Incident. Nothing herein prohibits either party from moving forward to notify regulatory authorities as may be required by law prior to notification of the other party so long as the notifying party provides notification to the other party without undue delay.

5.4 Transfers of Personal Data.

a. General Obligations for Transfer of Data. Either party may transfer personal data to third countries if such transfer complies with the provisions for the transfer of such data set forth in Applicable Data Protection Law. To the extent 5.4.c applies below, Customer represents that they are able to act as an exporting controller of data whether by their organisation being within the European Union or by being subject to categorization under Clause 13(a) of the SCCs as an organization capable of acting as an exporter from the European Union.

b. Transfers of EEA Personal Data to Customer. To the extent that Unity transfers personal data subject to EU Data Protection Law to Customer and Customer is established in a country outside of the EEA that is not subject to an adequacy decision, then Customer will be deemed to have entered into the required SCCs as the data importer with the Unity Party as identified in section 2.22 above as the data exporter, and such transfers will be subject to those SCCs.

c. Transfers of EEA Personal Data to Unity. To the extent that Customer transfers personal data subject to EU Data Protection Law to Unity, then Customer will be deemed to have entered into the required SCCs as the data exporter with Unity Party as identified in section 2.22 above , as the data importer, and such transfers will be subject to those SCCs.

d. Transfers of Brazilian Personal Data. To the extent that a party transfers personal data subject to the LGPD to the other party, then the transferring party will be deemed to have entered into the required SCCs as the data exporter with the receiving party as the data importer, and such transfers will be subject to those SCCs. With respect to Unity, such SCCs shall be deemed to be entered into by the Unity Party as identified in section 2.22above.

e. Transfers of Swiss Personal Data To the extent that a party transfers personal data subject to the Switzerland Data Protection Law, the 2021 Standard Contractual Clauses

form part of this DPA and take precedence over the rest of this DPA for such transfer to the extent of any conflict

f. Transfers of Personal Data from Argentina to outside of Argentina To the extent that provision of the Services involves the transfer of personal data from Argentina to outside of Argentina (either directly or via onward transfer) to a jurisdiction that does not have adequate legislation in the terms of article 12 of Law No. 25,326 and its regulatory Decree No. 1558/01, then the parties will be deemed to have entered into the required Argentinian Model Clauses, and such transfers will be subject to those Model Clauses. The roles of the parties and the description of transfers, for the purposes of Annex A to the Argentinian Model Clauses, is set out in Appendix A.

6. Controller-Processor Terms. The Controller-Processor Terms set forth in this Section 6 will apply only in connection with Customer's use of the Processor Services and Unity's processing of personal data in connection therewith.

6.1 Processing of Customer Personal Data

6.1.1 Relationship of the Parties. The parties acknowledge and agree that with regard to the processing of personal data for Processor 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 and that such controller is organised in the European Union and capable of acting as a data exporter or is acting upon the instruction of a controller that is or is otherwise categorized as a qualified exporter under Clause 13(a) of the SCCs.

6.1.2 Customer's Instructions. For the purposes of this DPA and, if applicable, the SCCs, Customer instructs Unity to process personal data for the following purposes: (i) to store and use data as described more fully in the Terms of Service and any applicable descriptions of the Processor Services (including, without limitation, Processing of ad revenue data associated with Partner Personal Data by Unity and/or Unity Affiliates for the purpose of providing the advertising Services by ironSource and/or ironSource Affiliates), (ii) to analyze data to maintain and improve the service, and (iii) to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms and conditions of the Terms of Service, this DPA, and Applicable Data Protection Law. 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 upon separately in a writing signed by authorized representatives of both parties.

6.1.3 Unity's Processing of Personal Data. In connection with Customer's use of the Processor Services, Unity will only process personal data on behalf of and in accordance with Customer's instructions 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, including any SCCs.

6.1.4 Security of Processing. 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. Such measures include those set forth in the Security, Privacy and Architecture Documentation. Unity will not materially decrease the overall security of the Services during the term of the Terms of Service.

6.1.5 Personal Data Breach Notification. Unity will notify you 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.

6.2 Compliance Assistance. To the extent required by Applicable Data Protection Law, Unity agrees to provide you with reasonable assistance in ensuring compliance with your obligations pursuant to Articles 32 to 36 of the GDPR and Articles 5, 6, 10, 38 and 46 of the LGPD, taking into account the nature of Unity's processing and the information available to Unity. Upon request from you, Unity will further provide commercially reasonable assistance to you by appropriate technical and organizational measures, insofar as this is possible, in relation to handling of a Data Subject's request for exercising Data Subject's rights set forth in Chapter III of the GDPR and Article 18 of the LGPD, taking into account the nature of Unity's processing of personal data and solely to the extent you are unable to fulfill such requests through the Services. You will be responsible for any costs arising from Unity's provision of such assistance.

6.3 Data Subject Requests. Notwithstanding the foregoing, if Unity receives a request from a data subject in relation to personal data, Unity will (a) if the request is made via a Compliance Tool, respond directly to the data subject's request in accordance with the standard functionality of the Compliance Tool, or (b) if the request is not made via a Compliance Tool, direct the data subject to submit his or her data subject request to Customer, and Customer will be responsible for responding to such request.

6.4 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.

6.5 Deletion of Customer Personal Data. Unity will delete all Customer personal data and copies thereof upon the request of Customer following termination or expiration of the Terms of Service unless otherwise required by Applicable Data Protection Law and/or Customer's instructions. The parties agree that the certification of the deletion of Customer personal data will be provided by Unity to Customer upon Customer's request at such times and in such manner as the Customer prescribes.

6.6 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. The parties agree that the audit rights described in Article 28 of the GDPR and, where applicable, as stipulated in the SCCs, will be satisfied by Unity's provision of such summaries and/or reports.

6.7 Unity Personnel

6.7.1 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.

6.7.2 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.

6.7.3 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.

6.8 Sub-Processors

6.8.1 General Authorization. To the extent required by Applicable Data Protection Law, you authorize 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. You agree that Unity has general written authorization to appoint sub-processors under Clause 9 of the SCCs.

6.8.2 New Sub-Processors. Unity will inform you of any intended changes concerning the addition or replacement of Sub-processors and provide you with five (5) business days to make reasonable objections to any new Sub-processors. In the event you reasonably object to a new Sub-processor, you may, as a sole remedy, terminate the applicable 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.

6.8.3 Sub-Processor Agreement. The parties agree that if copies of Unity's agreements with a Sub-Processor must be sent by Unity to Customer pursuant to Applicable Data Protection Law, such copies may have all commercial information and provisions unrelated to this DPA redacted by Unity beforehand; and, that such copies will be provided by Unity only upon reasonable request by Customer.

6.9 Transfers of Personal Data

6.9.1 General Obligations for Transfer of Data. Either party may transfer personal data to third countries if such transfer complies with the provisions for the transfer of such data set forth in Applicable Data Protection Law.

6.9.2 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, including any SCCs. Unity may enter agreements as necessary to fulfill the requirements laid down herein.

6.9.3 Transfers of EEA Personal Data to Unity. To the extent that Customer transfers personal data subject to EU Data Protection Law to Unity, then Customer will be deemed to have entered into the required SCCs as the data exporter with the Unity Party as identified in section 2.22 above as the data importer, and such transfers will be subject to those SCCs.

6.9.4 Transfers of Brazilian Personal Data to Unity. To the extent that Customer transfers personal data subject to the LGDP to Unity, then Customer will be deemed to have entered into the required SCCs as the data exporter with the Unity Party as identified in section 2.22above as the data importer, and such transfers will be subject to those SCCs.

6.9.5 Transfers of Swiss Personal Data To the extent that a party transfers personal data subject to the Switzerland Data Protection Law, the 2021 Standard Contractual Clauses form part of this DPA and take precedence over the rest of this DPA for such transfer to the extent of any conflict

6.9.6 Transfers of Personal Data from Argentina to outside of Argentina To the extent that the provision of the Services involves the transfer of Personal Data from Argentina to outside of Argentina (either directly or via onward transfer) to a jurisdiction that does not have adequate legislation in the terms of article 12 of Law No. 25,326 and its regulatory Decree No. 1558/01, then Customer will be deemed to have entered into the required Argentinian Model Clauses as the data exporter with the Unity Party as identified in section 2.22 above as the data importer, and such transfers will be subject to those Model Clauses. The description of transfers, for the purposes of Annex A to the Argentinian Model Clauses, is set out in Appendix A.

7. **Changes to this DPA**.

7.1 Unity may update the terms of this Addendum, including the designation of Controller Services and Processor Services in Section 3, from time to time, including, but not limited to: (a) as set forth in the applicable Unity Terms of Service ; (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 Non-Applicable Data Protection Law. If such 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, or to obtain the consent of the Customer if required under applicable law. 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.

8. Additional Terms for Non-Applicable Data Protection Laws

8.1 The parties acknowledge that data protection laws in addition to Applicable Data Protection Law may apply to the parties' processing of personal data.

8.2 **Japan**. This Section of this DPA 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.” Terms not otherwise defined in Section 2 shall have the meaning ascribed to it by the Japanese Data Protection Laws.

8.2.1 Controller Services. To the extent Controller Services listed under Section 3.1 are subject to Japanese Data Protection Laws, Unity, as a Business Operator Handling Personal Information, is responsible for the handling of Personal Information or Personal Data in its possession. Customer is responsible for providing any consents and notices required to permit (a) Customer's use and receipt of the Controller Services and (b) Unity’s 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.

8.2.1.1 Purpose of Use**.** The Customer shall permit Unity to utilize the Personal Information or Personal Data within the scope of the Permitted Purpose as stated under Section 5.2 Purpose of Processing.

8.2.1.2 Compliance. Unity and the Customer shall warrant that the necessary proceedings under the Japanese Data Protection Laws have been implemented, including, without limitation, (i) the recording of any transfer of Personal Data or Personally Referable Information to a Third Party or receipt of Personal Data from a Third Party and (ii) disclosing, correcting, adding or deleting the contents of, ceasing utilization of, erasing, or ceasing the third-party provision of Retained Personal Data or other relevant information upon the request from the data subjects, when meeting the requirements under the Japanese Data Protection Laws.

8.2.1.3 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.

8.2.1.4 In the case that the Customer provides Personal Information or Anonymously Processed Information, or Pseudonymously Processed Information or Personally Referable 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.

8.2.1.4.1 Unity shall, if the data have been provided in accordance with Section 8.2.1.4, comply with Japanese Data Protection Laws and take any measures required thereof for the management of the applicable data.

8.2.1.4.2 If the Personally Referable Information is to become Personal Data to Unity, Customer shall confirm that Unity has obtained consent from the data subjects or obtain such

consent from the data subjects on Unity's behalf when it provides the Personally Referable Information to Unity.

8.2.1.5 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.

8.2.2 Processor Services. To the extent that Processor Services listed under Section 3.2 is 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 the trustees including subcontractor to ensure the proper security management of the Personal Information or Personal Data.

8.2.2.1 Customer is responsible for providing any consents and notices required to permit (a) Customer's use and receipt of the Processor's Services and (b) Unity's 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.

8.2.2.2 To the extent required by Japanese Data Protection Laws, Sections 8.2.1.1 to 8.2.1.5 are incorporated by reference as if fully stated forth herein.

8.3 **South Korea.** This Section of this DPA 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 Section 2 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, guidance's and codes of practices issued by the regulatory bodies of South Korea. Hereinafter referred to "Korean Data Protection Laws."

8.3.1 To the extent Controller Services listed under Section 3.1 is subject to Korean Data Protection Laws the Customer is solely responsible for obtaining any consents and giving any notices required to permit (a) Customer's use and receipt of the Services and (b) Unity's 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 for such third party provision and/or international data transfer as contemplated under this DPA if and to the extent required under the Korean Data Protection Laws.

8.3.1.1 The Customer shall permit Unity to utilize the Personal Information within the scope of the Permitted Purpose as stated under Section 5.2 Purpose of Processing.

8.3.1.2 Unity and the Customer shall warrant that the proceedings under the Korean Data Protection Laws have been implemented.

8.3.1.3 Unity and the Customer shall comply with Korean Data Protection Laws and take necessary measures for the management of Personal Information.

8.3.1.4 In the case that the Customer provides data containing personal information, Anonymized, or Pseudonymized Information under the Korean 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 Anonymized or Pseudonymized Information to Unity in effecting the Permitted Purpose, the Customer shall warrant that the proceedings under the Korean Data Protection Laws have been implemented with respect to Anonymized or Pseudonymized Information.

8.3.1.4.1 Unity shall, if the data have been provided in accordance with Section 8.3.1.4, comply with Korean Data Protection Laws and take any measures required for the management of the data.

8.3.1.5 Unity shall at all times implement appropriate technical and organizational measures designed to safeguard Personal Information as required by Korean Data Protection Laws.

8.3.2 To the extent that Processor Services listed under Section 3.2 is 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 services listed under Section 3.2.

8.3.2.1 Service Provider shall perform personal information processing for the Processor Services listed under Section 3.2 in accordance with the terms and conditions of this DPA.

8.3.2.2 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.

8.3.2.3 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).

8.3.2.4 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 DPA as 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.

8.3.2.5 The Customer may supervise Service Provider in connection with the following matters, and Service Provider shall reasonably comply with such supervision:

- Status of the personal information processing;
- Status of those who can access the personal information and access logs thereof;
- Compliance of the provisions prohibiting use or third party transfer of the personal information outside the scope of the intended purpose or re-entrustment;
- Enforcement of measures necessary for securing safety such as encryption, etc.; and
- Other matters necessary for the protection of the personal information.

8.3.2.6 The Customer may reasonably request documentation to inspect the status of the matters set forth in Section 8.3.2.5 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.

8.3.2.7 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.

8.3.2.8 The details of the training under Section 8.3.2.7 above, including the time and method, shall be implemented upon consultation between the Customer and Service Provider as necessary.

8.3.2.9 Either party shall indemnify the other party, data subject or any third party for any damages due to the breach of this Section 8.3 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.

8.3.2.10 With respect to Section 8.3.2.9 above, 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.

8.4 **Singapore**. This Section of this DPA 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 Section 8.4 shall have the meaning ascribed to it by the Singapore Data Protection Laws

8.4.1 To the extent Controller Services listed under Section 3.1 are subject to Singapore Data Protection Laws, Customer is responsible for any consents and notices required to permit (a) Customer's use and receipt of the Controller Services and (b) Unity's accessing, storing, and processing of data provided by Customer (including Personal Data, if applicable) under the Terms of Service and this DPA. Additionally, Customer agrees to obtain the consent of each Data Subject to an International Data 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 Controller Services under the Terms of Service.

8.4.1.1 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 as stated under Section 5.2 Purpose of Processing of fulfilling its obligations and providing the services required under the Terms of Service; 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

8.4.1.2 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 remain 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.

8.4.1.3 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.

8.4.1.4 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.

8.4.1.5 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.

8.4.1.6 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.

8.4.1.7 In the case that the Customer provides Personal Information or Anonymously Processed Information under Singapore Data Protection Laws to Unity in effecting the Purpose, the Customer shall specify that effect in advance. In the case that the Customer provides Anonymously Processed Information to Unity in effecting the Purpose, the Customer shall warrant that the proceedings under the Singapore Data Protection Laws have been implemented with respect to the Anonymously Processed Information.

8.4.1.7.1 Unity shall, if the data have been provided in accordance with Section 8.4.1.7, comply with Singapore Data Protection Laws and take any measures required for the management of the data.

8.4.2 To the extent that Processor Services listed under Section 3.2 is 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

8.4.2.1 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's 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.

8.4.2.1.1 Sections 8.4.1.2 to 8.4.1.6 are incorporated by reference as if fully said forth herein.

8.5 **China**. This Section of this DPA 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 by Personal Information Protection Law of People's Republic of China ("PIPL"), including where applicable, rules, guidance and codes

of practices issued by the regulatory bodies of China hereinafter, "Chinese Data Protection Laws". Terms not otherwise defined in Section 8.5 shall have the meaning ascribed to it by the Chinese Data Protection Laws.

8.5.1 Controller Services. To the extent Controller Services listed under Section 3.1 are subject to Chinese Data Protection Laws, Unity, as the Personal Information Handler, is responsible for the handling of Personal Information in its possession. Customer is responsible for any consents and notices required to permit (a) Customer's use and receipt of the Controller Services and (b) Unity's accessing, storing, and processing of Personal 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 Data Transfer as contemplated under this DPA if and to the extent required under the Chinese Data Protection Laws. Personal Information may be transferred, as necessary, world-wide to provide the Controller Services under the Terms of Service.

8.5.1.1 The Customer acknowledges and agrees that the Controller Services have the function to process Personal Information and agrees that the processing of Personal Information is for the necessity of providing the services. The Customer shall permit Unity to utilize the Personal Information within the scope of the Permitted Purpose as stated under Section 5.2 Purpose of Processing.

8.5.1.2 Unity and the Customer shall comply with the Chinese Data Protection Laws and take necessary measures for the handling, and transfer of Personal Information, including without limitation, any procedures, security assessment, certifications, standard contract required by the Chinese Data Protection Law.

8.5.1.3 The Customer shall clearly inform its End User through its privacy policy or other documents includes but not limited to: (a) the type of Personal Information processed by the Customer, the purpose, the processing method, the retention period, etc; (b) the Customer has chosen Unity as its service provider, Customer has used Unity's Controller Services; (c) that Unity will process Personal Information and transfer Personal Information outside of China in accordance with Unity's China Privacy Policy (with an URL to this policy); and (d) any other information required by the Chinese Data Protection Laws.

8.5.1.4 The Customer acknowledges that neither Unity nor Unity's Affiliate has established direct contractual relationship with End Users. Therefore Customer warrants that it has provided appropriate notices to obtain valid and separate consents from End Users with regard to the handling of Personal Information by Unity and International Data Transfer contemplated under this DPA.

8.5.2 Processor Services. To the extent that Processor Services listed under Section 3.2 is subject to Chinese Data Protection Law, the Customer acknowledges that Unity is a not a Personal Information Handler with respect to the Processor Services listed under Section 3.2, but an Agent of the Customer under the PIPL. The Customer agrees to entrust Unity an Agent and

Unity hereby agrees to provide the processing of Personal Information with respect to the Processor Services listed under Section 3.2.

8.5.2.1 Unity will only process Personal Information on behalf of and in accordance with Customer's instructions and otherwise in accordance with the requirements of Chinese Data Protections Laws.

8.5.2.2 Unless with the Customer's prior consent, Unity may not re-entrust third party to process the Personal Information related to the Processor Services listed under Section 3.2.

8.5.2.3 The Customer shall permit Unity to utilize the Personal Information and engage subcontractor in accordance with Section 6. Unity, as the Agent, will not handle the Personal Information beyond the agreed purpose and method of handling. The Customer may exercise necessary and appropriate supervision of the Agent including the permitted subcontractor to ensure the proper security management of the Personal Information.

8.5.2.4 The Customer is responsible for any consents and notices required to permit (a) Customer's use and receipt of the Processor Services listed under Section 3.2; and (b) Unity's 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 as required by the Chinese 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.

8.5.2.5 Section 8.5.1.2 and Section 8.5.1 4 are incorporated by reference as if fully said forth herein

CUSTOMER

Signature:_____

Print Name:_____

Title:_____

Date:_____

UNITY TECHNOLOGIES S.F.

Signature: DocuSigned by: Jamie Crabtree 5D82CA382BAD4B9...

Print Name: Jamie Crabtree

Title: DPO

Date: March 29, 2023

Appendix A

FOR CONTROLLER SERVICES - MODULE ONE TRANSFER CONTROLLER TO CONTROLLER

ANNEX I- Controller Controller Services

A. LIST OF PARTIES

Data exporter(s):
Name: _____ i.e., Customer, as identified in the applicable Offering Identification and/or Customer's Service Account

Address: _____ i.e., Customer's address, as identified in the applicable Offering Identification and/or Customer's Service Account

Contact person's name, position and contact details :_____ i.e., Customer's point of contact, as identified in the applicable Offering Identification and/or Customer's Service Account

Activities relevant to the data transferred under these Clauses: _____ i.e., Storing and analyzing data to carry out the purposes of the data transfer

Date: Deemed signed and effective as of the effective date set forth in the applicable Offering Identification or the date on which Customer started to use a Unity service, whichever is earlier.

Signature:_____

Role (controller/processor): Controller

Data importer(s):
Name: Unity Party as identified in section 2.22 above

Address:

- Unity Technologies S.F., 30 3rd Street, San Francisco, CA 94103

Contact person's name, position and contact details: Jamie Crabtree; DPO; dpo@unity3d.com

Activities relevant to the data transferred under these Clauses: Storing and analyzing data to carry out the purposes of the data transfer

Date: Deemed signed and effective as of the effective date set forth in the applicable Offering Identification or the date on which Customer registered for any of the Unity Services or otherwise accessed, enabled or utilized any of the Unity Services or Unity Assets, whichever is earlier.

Signature: DocuSigned by: Jamie Crabtree 5D82CA382BAD4B9...

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Data subjects may include Customers, Partners, and Vendors (including without limitation employees/ staff) and their end users about whom Personal Data is provided to Unity via the Services by, or at the direction of, Customer.

Categories of personal data transferred

- Information processed through the customer's use of the services including contact information, device information, information uploaded by the customer, location information, financial information, software usage event information, authentication information (including tokens), and IP address. This includes usernames of employees who access Unity's ordering system to place advertisements, bid on the right to advertise to any End User, or any vendor employee who provides such information to Unity in performing services for Unity.
- End Users data including voice, advertising identifiers or device IDs (e.g. IDFA GAID), User IDs, IP address, game play, in-app purchase, and device data, including device identifiers,
- Information related to the ad content or attribution data sent by Customer or Customer's agent

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.

- Biometric data may be transferred through the use of Safe Voice.
- Unity shall secure Biometric Information in the same manner as any other confidential or sensitive information that it stores, including stringent access restrictions with limited permissions based on roles, access audits and security reviews. The information shall be destroyed upon conclusion of its use as specified elsewhere in this DPA.

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

- Transferred continuously

Nature of the processing

- To provide the Services in accordance with the Terms of Service, or with instructions from the User (including instructions provided through the User's Account).

Purpose(s) of the data transfer and further processing

- To provide the Services in accordance with the Terms of Service, or with instructions from the User (including instructions provided through the User's Account).
- For end users, the data may be transferred to personalize advertising and in game purchase opportunities as well as to personalize game play.
- To facilitate, support and operate games and player or user experiences
- Analytics to maintain and improve the service
- For Unity's internal purposes, including billing and payment processing, fraud prevention, and improving products and services.

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

Unity retains personal data for as long as needed or permitted in light of the purpose(s) for which it was obtained and consistent with applicable law. The criteria used to determine our retention periods include:

- The length of time Unity has an ongoing relationship with the data subject and/or Customer, including the provision of provision of services;
- Whether there is a legal obligation to which Unity is subject;
- Whether retention is advisable in light of our legal position

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

- Unity uses processors as necessary to perform the Services pursuant to the Terms of Service on a continuous basis for the duration of the retention period.

C. COMPETENT SUPERVISORY AUTHORITY

Unity's Competent Supervisory Authority is the Danish Data Protection Agency, Carl Jacobsens Vej 35, DK-2500 Valby; dt@datatilsynet.dk; +45 33 19 32 00

D. ELECTIONS UNDER EU SCCS

1. Clause 7 Docking Clause: This optional clause allowing, with the agreement of the Parties, for an entity that is not a Party to these Clauses to accede to these Clauses at any time shall apply.
2. Clause 9 (a) Use of sub-processors: N/A for Module One
3. Clause 11 (a) Redress: This optional clause allowing for the appointment of an independent dispute resolution body to receive complaints by the data subjects shall not apply.
4. Clause 13 (a) Supervision:
    a. 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, as indicated in Annex I.C, shall act as competent supervisory authority.
    b. 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, as indicated in Annex I.C, shall act as competent supervisory authority.
    c. 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: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

5. Clause 17 Governing Law: Option One allowing for these Clauses to be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law provided for in Section 4.8 above.
6. Clause 18 (b) Choice of Forum and Jurisdictions: The Parties agree that any dispute arising from these Clauses shall be resolved by the courts provided for in Section 4.8 above.

E. ELECTIONS UNDER THE UK SCCS

The Information Commissioner's Office International Data Transfer Addendum To The EU Commission Standard Contractual Clauses shall be deemed incorporated by reference to this DPA.

1. The Parties and Selected SCCs, Modules and Selected Clauses have been identified in this ANNEX I above.
2. Either Importer or Exporter may end the Addendum as set out in Section 19 of the Addendum i.e.:
    - 19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
        - a its direct costs of performing its obligations under the Addendum;and/or
        - b its risk under the Addendum,

      and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum

F ELECTIONS UNDER SWISS SCCS

The SCCs will be deemed completed in accordance with this Annex 1 except that:

1. Under Clause 13 of the EU SCCs, the competent supervisory authority is the Swiss Federal Data Protection and Information Commission to the extent that the transfer is governed by the Swiss Federal Act on Data Protection,
2. References to "Member State" in the 2021 Standard Contractual Clauses refer to Switzerland, and data subjects may exercise and enforce their rights under the 2021 Standard Contractual Clauses in Switzerland.
3. References to GDPR in the 2021 Standard Contractual Clauses refer to the Swiss Federal Act on Data Protection (as amended and replaced).

[and/or]

FOR PROCESSOR SERVICES - MODULE TWO TRANSFER CONTROLLER TO PROCESSOR

ANNEX I to Controller-Processor SCCs

A. LIST OF PARTIES

Data exporter(s):

Name: _____ i.e., Customer, as identified in the applicable Offering Identification and/or Customer's Service Account,

Address: _____ i.e., Customer's address, as identified in the applicable Offering Identification and/or Customer's Service Account

Contact person's name, position and contact details: _____ i.e., Customer's point of contact, as identified in the applicable Offering Identification and/or Customer's Service Account

Activities relevant to the data transferred under these Clauses: Oversight of common data protection program to assure uses of the transferred data are limited to the uses described herein.

Date: Deemed signed and effective as of the effective date set forth in the applicable Offering Identification or the date on which Customer registered for any of the Unity Services or otherwise accessed, enabled or utilized any of the Unity Services or Unity Assets, whichever is earlier.

Signature:_____

Role (controller)/processor): Controller

Data importer(s):

Name: Unity Party as identified in section 2.22 above

Address:

- Unity Technologies S.F., 30 3rd Street, San Francisco, CA 94103

Contact person's name, position and contact details: Jamie Crabtree, DPO dpo@unity3d.com

Activities relevant to the data transferred under these Clauses: Oversight of common data protection program to assure uses of the transferred data are limited to the uses described herein.

Date: Deemed signed and effective as of the effective date set forth in the applicable Offering Identification or the date on which Customer registered for any of the Unity Services or otherwise accessed, enabled or utilized any of the Unity Services or Unity Service Assets, whichever is earlier.

Signature: DocuSigned by: Jamie Crabtree 5D82CA382BAD4B9...

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Data subjects may include Customers, Partners, and Vendor (including without limitation employees/ staff) end users about whom Personal Data is provided to Unity via the Services by, or at the direction of, Customer.

Categories of personal data transferred

- Information processed through the Customers use of the services including contact information, device information, information uploaded by the customer, location information, financial information, software usage event information, authentication information (including tokens), and IP address. This includes usernames of employees who access Unity's ordering system to place advertisements, bid on the right to advertise to any End User, or any vendor employee who provides such information to Unity in performing services for Unity.
- End Users data including voice, advertising identifiers or device IDs (e.g. IDFA GAID), User IDs, IP address, game play, in-app purchase, and device data, including device identifiers,
- Information related to the ad content or attribution data sent by Customer or Customer's agent

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.

- Biometric data may be transferred through the use of Ziva Face Trainer, Unity MARS,Unity AR Companion App
- Unity shall secure Biometric Information in the same manner as any other confidential or sensitive information that it stores, including stringent access restrictions with limited permissions based on roles, access audits and security reviews. The information shall be destroyed upon conclusion of its use as specified elsewhere in this DPA.

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

- Transferred continuously

Nature of the processing

- To provide the Services in accordance with the Agreement or Terms of Service, or with instructions from the User (including instructions provided through the User's Account).

Purpose(s) of the data transfer and further processing

- For game players, the data is transferred for in-game purchase opportunities as well as to personalize game play, such as through IAP and Remote Config Services.
- To facilitate, support and operate games and player or user experiences
- To provide the Services in accordance with the Agreement or Terms of Service, or with instructions from the User (including, without limitation, Processing of ad revenue data associated with Partner Personal Data by Unity and/or Unity Affiliates for the purpose of providing the advertising Services by Unity and/or Unity, and instructions provided through the User's Account).
- Analytics to maintain and improve the service
- For Unity's internal purposes, including billing and payment processing, fraud prevention, and improving products and services.

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

Unity retains personal data for as long as needed or permitted in light of the purpose(s) for which it was obtained and consistent with applicable law. The criteria used to determine our retention periods include:

- The length of time Unity has an ongoing relationship with the data subject and/or Customer, including the provision of services;
- Whether there is a legal obligation to which Unity is subject;
- Whether retention is advisable in light of our legal position

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

- Unity uses processors as necessary to perform the Services pursuant to the Agreement on a continuous basis for the duration of the retention period.

C. COMPETENT SUPERVISORY AUTHORITY

Unity's Competent Supervisory Authority is the Danish Data Protection Agency, Carl Jacobsens Vej 35, DK-2500 Valby; dt@datatilsynet.dk; +45 33 19 32 00

List of sub-processors available inside of your account settings page, or upon request to DPA@unity3d.com

.D. TECHNICAL AND ORGANISATIONAL MEASURES

Available upon request to DPA@unity3d.com

E. ELECTIONS UNDER EU SCCS

1. Clause 7 Docking Clause: This optional clause allowing, with the agreement of the Parties, for an entity that is not a Party to these Clauses to accede to these Clauses at any time shall apply.
2. Clause 9 (a) Use of sub-processors: Option 2 allowing for General Written Authorization for the engagement of sub-processor(s) shall apply via the mechanism specified in Section 6.8 above.
3. Clause 11 (a) Redress: This optional clause allowing for the appointment of an independent dispute resolution body to receive complaints by the data subjects shall not apply.
4. Clause 13 (a) Supervision:
    a. 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, as indicated in Annex I.C, shall act as competent supervisory authority.
    b. 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, as indicated in Annex I.C, shall act as competent supervisory authority.

c. 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: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

5. Clause 17 Governing Law: Option One allowing for these Clauses to be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law provided for in Section 4.8 above.
6. Clause 18 (b) Choice of Forum and Jurisdictions: The Parties agree that any dispute arising from these Clauses shall be resolved by the courts provided for in Section 4.8 above.

F. ELECTIONS UNDER THE UK SCCS

The Information Commissioner's Office International Data Transfer Addendum To The Eu Commission Standard Contractual Clauses shall be deemed incorporated by reference to this DPA.

1. The Parties and Selected SCCs, Modules and Selected Clauses have been identified in this ANNEX I above.
2. Either Importer or Exporter may end the Addendum as set out in Section 19 of the Addendum i.e.:
    - 19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
        - a its direct costs of performing its obligations under the Addendum;and/or
        - b its risk under the Addendum,

      and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum

G ELECTIONS UNDER SWISS SCCS

The SCCs will be deemed completed in accordance with this Annex 1 except that:

1. Under Clause 13 of the EU SCCs, the competent supervisory authority is the Swiss Federal Data Protection and Information Commission to the extent that the transfer is governed by the Swiss Federal Act on Data Protection,
2. References to "Member State" in the 2021 Standard Contractual Clauses refer to Switzerland, and data subjects may exercise and enforce their rights under the 2021 Standard Contractual Clauses in Switzerland.
3. References to GDPR in the 2021 Standard Contractual Clauses refer to the Swiss Federal Act on Data Protection (as amended and replaced).