APPLOVIN DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is incorporated into and is subject to the AppLovin Terms of Use Agreement available at https://www.applovin.com/terms or other applicable offline agreement (the "**Agreement**") between AppLovin Corporation and User. To the extent you are using the Services, you shall be deemed to have accepted this DPA upon acceptance or execution of the applicable Agreement.

1. SCOPE

1.1 User enters into this DPA on behalf of itself and on behalf of its authorized Affiliates. AppLovin may disclose Personal Data through User's use of the Services and the Parties agree to comply with the following provisions with respect to any Personal Data processed in connection with the Services.

2. DEFINITIONS

In addition to the terms defined in the Agreement and above, the following terms shall have the following meanings for the purposes of this DPA:

2.1 "**Adequate Jurisdiction**" means a country which ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data, as determined by the European Commission in the case that GDPR applies, and as determined by the UK Information Commissioner's Office in the case that the UK GDPR applies.

2.2 "**Affiliates**" means an entity that directly or indirectly controls, is controlled by, or is under common control with, a Party.

2.3 "**CCPA**" means the California Consumer Privacy Act of 2018, Cal Civ. Code §1798.100 et seq., and all implementing regulations, as amended from time to time, such as by the California Privacy Rights Act of 2020 ("CPRA").

2.4 "**Data Protection Laws**" means EU Data Protection Law, the CCPA, the Brazilian General Personal Data Protection Law, No. 13,709/2018 (the "**LGPD**"), and any other legislation protecting natural persons' right to privacy with regard to the processing of Personal Data to the extent applicable to a Party's Processing of Personal Data in connection with the Services.

2.5 "**Data Subject Rights**" means the rights granted to Data Subjects under Data Protection Laws.

2.6 "**EU Data Protection Law**" means the GDPR, the e-Privacy Directive and national implementing legislation and the Swiss Federal Data Protection Act.

2.7 "**GDPR**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("**EU GDPR**") and, where applicable, the "**UK GDPR**" as defined in the Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit) Regulations 2019.

2.8 "**Member State**" means a member state of the European Economic Area, together with Switzerland and the United Kingdom.

2.9 "**SCCs**" means (a) Module 1 (*controller to controller*) of the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 (the "**EU SCCs**"); (b) Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses (as such terms are defined in that Approved Addendum) (the “**UK Mandatory Clauses**”), together with any other necessary conforming changes to the EU SCCs (collectively, the “**UK SCCs**”); and (c) any updated, revised, or separate clauses relating to data transfer requirements of the GDPR issued from time to time by the European Commission, UK Information Commissioner’s Office, any other applicable data protection authority, or other body with competent authority and jurisdiction.

2.10 "**Shared Personal Data**" means Personal Data Processed by a Party to the extent such Party received that Personal Data from the other Party (that other party, the “**Sharing Party**” under this definition) in connection with the performance of the Agreement. For the avoidance of doubt, a Party is also deemed to “receive” Personal Data from a Sharing Party where the Sharing Party grants access to such Personal Data to the receiving Party.

2.11 "**Transparency Notices**" has the meaning given to it in clause 3.2(a).

2.12 The terms "**Controller**," “**Process**,” "**Processor**," "**Data Subject**," and "**Personal Data**," shall have the meanings given in EU Data Protection Law. To the extent Data Protection Laws use different terms to cover concepts similar to those covered under the aforementioned bold terms in this Section 2.12, then "**Controller**," “**Process**,” "**Processor**," "**Data Subject**,” and "**Personal Data**" shall have the meaning assigned to those different terms under such Data Protection Laws.

3. DATA PROCESSING; INDEPENDENT CONTROLLERS

3.1 AppLovin and User: (a) are independent Controllers with regard to the Shared Personal Data; and (b) will individually determine the purposes and means of its processing of Personal Data.

3.2 Each Party shall, with respect to the Processing of any Shared Personal Data, comply with Data Protection Laws, including as follows:

(a) each Party shall provide all applicable notices to Data Subjects as required under Data Protection Laws for the lawful Processing by it of Shared Personal Data ("**Transparency Notices**"). As required under Data Protection Laws, User shall disclose its use of the Services and how AppLovin Processes Personal Data in its Transparency Notices.

(b) each Party shall provide all required mechanisms for, and give effect to, applicable Data Subject Rights pursuant to Data Protection Laws and respond to inquiries by governmental authorities.

(c) User shall not disclose Shared Personal Data with any third parties except as expressly permitted under the Agreement. Further, User shall delete all Shared Personal Data promptly upon the occurrence of any of the following: (i) where User does not place the winning bid for an impression to which that Shared Personal Data relates or (ii) after User provides an Advertisement (directly or indirectly, such as via a third-party ad server in the latter case) in response to an ad request to which that Shared Personal Data relates. Without limiting the foregoing, User shall not, and shall not permit any third party to, use any Shared Personal Data in connection with any profiling or tracking of any end user or any other Data Subject or of any Mobile Property or Publisher.

(d) neither Party shall Process the Shared Personal Data for any purpose other than as set out in its Transparency Notice and unless such Processing is also authorised under Data Protection Laws and the Agreement.

(e) each Party shall ensure that all of its employees engaged in the Processing of such Shared Personal Data act consistently with this DPA.

(f) each Party shall implement technical and organisational security measures to prevent (i) the accidental, unlawful, or unauthorized destruction, loss, alteration, or disclosure of, or access to, Shared Personal Data or (ii) any other security incident that amounts to a "personal data breach" (as such term or similar term, such as "breach of the security system" or "data breach," is defined under Data Protection Laws) of Shared Personal Data (in either case of (i) and (ii), a "**Data Breach**").

(g) each Party agrees that any agreement with a subprocessor shall comply with the Data Protection Laws.

3.3 Each Party shall in particular, unless prohibited under applicable law, notify the other without undue delay (i) of any requests to exercise Data Subject Rights received by that Party regarding the Shared Personal Data, to the extent such notices are required under Data Protection Law; (ii) about regulatory inquiries involving the Processing of Shared Personal Data, and (iii) any Data Breach involving the Shared Personal Data to the extent resulting in material destruction, loss, alteration, or disclosure of, or access to, that Shared Personal Data.

3.4 Without limitation of the obligations and restrictions otherwise set forth in this DPA and elsewhere in the Agreement, each Party shall provide all required notices to, and obtain all necessary permissions and consents from, the relevant Data Subjects whenever required under the Data Protection Laws to lawfully permit such Party's Processing of Shared Personal Data in its capacity as an independent Controller of the Shared Personal Data.

3.5 User shall honor, in compliance with Applicable Data Protection Laws and applicable self-regulatory frameworks, all signals that AppLovin sends to User regarding whether the Data Subject has provided, or has not provided (or has withdrawn), consent or opted out of "sales" or "shares" (as such terms "sale" and "share" are defined under the Data Protection Laws and CCPA, respectively) or any similar signals (e.g., an opt out of targeted advertising).

3.6 With respect to the CCPA, (i) without limitation of any other restrictions set forth in the Agreement, the Shared Personal Data is disclosed to User for the limited and specified purposes of enabling User to bid on advertising inventory or serve Advertisements through the Services and User shall Process the Shared Personal Data only for such purposes; (ii) User shall comply with the CCPA, including by providing the same level of privacy protection as required of Controllers under the CCPA; (iii) AppLovin may take reasonable and appropriate steps to ensure that User Processes Shared Personal Data in a manner consistent with AppLovin's obligations under the CCPA; (iv) User shall notify AppLovin promptly after User makes a determination that it can no longer meet its obligations under the CCPA; and (v)

AppLovin may, upon notice, take reasonable and appropriate steps to stop and remediate the unauthorized Processing of Shared Personal information.

4. GENERAL

4.1 In the event of any conflict or discrepancy between the SCCs, the Agreement, and this DPA, the following order of precedence will apply: (i) the SCCs, (ii) this DPA, and (iii) the Agreement.

4.2 This DPA does not alter the limitations of liability set out in the Agreement.

4.3 This DPA will become effective on the date User has accepted the Agreement or the date on which the User started to use the Services. This DPA will terminate simultaneously and automatically upon the termination or expiration of the Agreement.

4.4 To the extent required by 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 Agreement.

5. INTERNATIONAL TRANSFERS

5.1 The Parties agree that the SCCs shall apply to the transfer of, including access to, Shared Personal Data in the case of a transfer from AppLovin to User, where:

(i) the User is not established in an Adequate Jurisdiction; and

(ii) the Processing of the Shared Personal Data is subject to EU Data Protection Law or the LGPD or AppLovin is otherwise contractually required to enter into the SCCs.

5.2 For the purposes of the SCCs:

(a) Annex 1.A (List of Parties) shall be deemed to incorporate the information in Schedule I;

(b) Annex 1.B (Description of Transfer) shall be deemed to incorporate the information in Schedule III;

(c) Annex 1.C (Competent Supervisory Authority) shall be deemed to refer to the supervisory authority identified in Schedule II;

(d) Annex II (Technical and Organisational Measures) shall be deemed to incorporate the information in Schedule II;

(e) The optional language within clause 7 of the SCCs does not apply;

(f) The optional language within clause 11(a) of the SCCs does not apply;

(g) Pursuant to clause 17, the SCCs will be governed by the laws of Ireland;

(h) Pursuant to clause 18(b) of the SCCs, the Parties shall resolve disputes under the SCCs before the courts of Cyprus;

(i) Table 4 referenced in the UK Mandatory Clauses is not applicable to either Party; and

(j) For data exporters established within Brazil (for purposes of transfers of Shared Personal Data under the LGPD), the SCCs shall be governed by the laws of the Federative Republic of Brazil. Further, for such transfers under the LGPD, the applicable Data Protection Law shall be understood as the LGPD and the supervisory authority is the National Data Protection Authority in Brazil (ANPD).

SCHEDULE I

PARTIES

Contractual party and Role	Address of the party, contact person's name, position and contact details and, where applicable, of its data protection officer and/or representative in the EU	Activities relevant to the data transferred under these Clauses
AppLovin **(Controller)**	AppLovin Corporation Address: 1100 Page Mill Road, Palo Alto, CA 94304 USA E-mail: dataprotection@applovin.com	Personal Data is transferred from AppLovin to the User in connection with the Services.
User **(Controller)**	As specified in the Agreement.	Personal Data that is made available to User in connection with the Services.

SCHEDULE II

SCCS

Information deemed incorporated into the SCCs	
Data exporter	AppLovin
Data importer	User
Annex I.A	**List of Parties**: Relevant information regarding “Data exporter” and “Data importer” under this Schedule I and Schedule II are incorporated by reference herein.
Annex I.B	**Description of Transfer**: Relevant information from Schedule III below is incorporated by reference herein**.**
Annex I.C	**Competent Supervisory Authority**: The competent supervisory authority shall be Cyprus’ Commission for the Protection of Personal Data *except that*, in the case of the UK SCCs, the competent supervisory authority under the UK SCCs will be the UK Information Commissioner.
Annex II	**Technical and Organisational Measures**: Data importer will implement and maintain appropriate administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of Shared Personal Data, including: **1. Measures for pseudonymization and encryption of Shared Personal Data:** A. Data minimization and privacy-by-design into its software or other product/service development lifecycle to prevent Shared Personal Data from being used in a manner inconsistent with the Agreement. For example, Data importer only works with pseudonymized data and has international controls to prohibit internal personnel and any relevant subprocessors from re-identifying data to any directly identifying Personal Data (e.g., name, address). B. User does not utilize sensitive Personal Data (e.g., “special categories of Personal Data” under the GDPR) or directly identifiable Personal Data in connection with its use of the Services. C. User utilizes appropriate, industry standard cryptography when storing Shared Personal Data (e.g., encryption at rest) and when utilizing hashed or other cryptographically protected identifiers, wherever feasible. **2. Measures for ensuring ongoing confidentiality of processing systems and services:** A. User has implemented and maintains a written information security program and has implemented measures to ensure the integrity, availability, and security of Personal Data, including regular vulnerability scans and endpoint protection. B. User has a documented data retention/deletion schedule that aligns with the retention/deletion requirements under the Agreement with respect to Shared Personal Data.

3. Measures for ensuring ongoing integrity of processing systems and services:

A. User has implemented and maintains a written information security program that contains administrative, technical, and physical safeguards appropriate to protect against potential Data Breaches and remediate actual or reasonably suspected Data Breaches, and that meet (i) industry best practices in relation to User’s industry and (ii) any security requirements required under Data Protection Laws.

4. Measures for ensuring ongoing availability and resilience of processing systems and services:

A. User maintains Shared Personal Data availability and resilience via its written information security program, such as via secured and monitored operational sites, event and other auditable logs, tolerant infrastructure with appropriate redundancies, processes and policies for incident response and vendor due diligence, business continuity plans, backup procedures, and disaster recovery plans.

5. Measures for ensuring the ability to restore the availability and access to Shared Personal Data in a timely manner in the event of a physical or technical event:

A. See above.

6. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing:

A. At least annually, security measures and the written information security program are reviewed and tested for alignment with the requirements herein and industry best practices.

B. Security compliance is integrated within User’s product/service development lifecycle and User’s teams collaborate regularly to ensure those standards are kept up to date.

7. Measures for user identification and authorization:

A. User has procedures in place to authenticate and respond to requests from Data Subjects who have submitted rights requests (e.g., access, portability, erasure), and such procedures comply with Data Protection Laws.

B. User has operational and technical controls in place to ensure appropriate system access control with respect to Shared Personal Data and related infrastructure, such that only authorized personnel are granted access based on a “need to know” (and that unauthorized current or former personnel cannot improperly access such systems).

8. Measures for the protection of Shared Personal Data during storage:

A. See above, and the Agreement more broadly, for limitations on how User can Process the Shared Personal Data.

B. User has implemented and maintains data minimization procedures with respect to Shared Personal Data stored on User’s, or its subprocessors, systems.

9. Measures for ensuring physical security of locations at which Shared Personal Data is

	Processed: A. Facilities involved in the Processing of Shared Personal Data are accessible only be authorized personnel and there are logical and physical controls in relation thereto (e.g., two-factor authentication, firewalls, anti-malware, access controls, VPNs, access badges and logs, physical barriers). **10. Measures for ensuring accountability** A. User has performed a data mapping exercise that is compliant with Data Protection Laws and has created an appropriate record of Processing activities in relation thereto. B. User has implemented a privacy program appropriate to the scope and nature of the Personal Data Processed, including, as applicable, reviewing and complying with self-regulatory frameworks where appropriate, conducting data protection impact assessments, and appointing a data protection officer (DPO) or other individuals responsible for privacy and data security as appropriate.

SCHEDULE III

DESCRIPTION OF THE TRANSFER

Categories of data subjects whose data is transferred
The personal data transferred concern the following categories of data subjects:

- Individuals who are the subject of a bid request sent from AppLovin to User or otherwise are served an impression.

Categories of data transferred
The personal data transferred concern the following categories of data:

Mobile device advertising identifiers (e.g., IDFA/Google Ad ID, IP address) or other digital/device identifiers

Device/user agent data such as make, model, operating system, device properties and settings, location data, application ID, and application version

Click and view (impression) data

Sensitive data transferred (if applicable)
The personal data transferred concern the following categories of sensitive data:

None.

The frequency of the transfer

The transfer will take place on a real-time, continuous basis pursuant to the Agreement

Nature of the processing and purpose of the transfer(s) and further processing

The Personal Data is Processed in connection with the use of the Services in accordance with the Agreement.

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

User will not retain the Shared Personal Data for longer than as permitted under the Agreement.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing
The Personal Data transferred may be disclosed only to the following recipients or categories of recipients:

Service providers that User uses in connection with the Services and those otherwise described in its Transparency Notice.
The duration of Processing will align with the data retention period described above.