Applovin Data Processing Agreement

This AppLovin Data Processing Agreement ("**DPA**") is incorporated into and is subject to the AppLovin Terms of Use Agreement available at https://www.applovin.com/terms (the "**Agreement**") entered into by and between User and AppLovin (as those terms are defined in the Agreement). This DPA reflects the parties' agreement with regard to the Processing of Personal Data. User and AppLovin are hereinafter jointly referred to as the "Parties" and individually as a "Party." This DPA shall apply to the Agreement to the extent User is established within the European Economic Area ("**EEA**"), the United Kingdom ("**UK**") or Switzerland and/or to the extent AppLovin Processes Personal Data of Data Subjects located in the EEA, the UK or Switzerland on behalf of User.

User enters into this DPA on behalf of itself, and to the extent required under applicable Data Protection Laws, in the name and on behalf of its authorized Affiliates, if and to the extent AppLovin Processes Personal Data for which such authorized Affiliate qualifies as the Data Controller. In the course of providing the Services to User pursuant to the Agreement, AppLovin may Process Personal Data on behalf of User and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith. References to the Agreement will be construed as including this DPA. Any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement.

1. **DEFINITIONS**

   In this DPA, the following terms shall have the meanings set out below:

   1.1 "**Affiliate**" means any entity which is controlled by, controls or is in common control with a Party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

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

   1.3 "**Data Processor**" means the entity which Processes Personal Data on behalf of the Data Controller.

   1.4 "**Data Protection Laws**" means the EU General Data Protection Regulation 2016/679 ("GDPR").

   1.5 "**Data Subject**" means the individual to whom Personal Data relates.

   1.6 "**Personal Data**" means any information relating to an identified or identifiable person.

   1.7 "**Privacy Shield**" means the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce.

   1.8 "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction ("Process", "Processes" and "Processed" shall have the same meaning).

   1.9 "**Security Breach**" has the meaning set forth in Section 7 of this DPA.

   1.10 "**Services**" means AppLovin's ad network enabling the purchase and sale of mobile advertising.

   1.11 "**Sub-processor**" means any Data Processor engaged by a Data Processor.

2. **PROCESSING OF USER PERSONAL DATA**

2.1   The Parties agree that with regard to the Processing of Personal Data, User is the Data Controller and AppLovin is the Data Processor.

2.2   User agrees to publicly post a privacy policy describing its Processing of Personal Data that complies with Data Protection Laws. User shall disclose its use of the Services and how AppLovin Processes Personal Data in its privacy policy. This can be done by including the following language in the User's privacy policy: "We work with AppLovin to deliver ads in our mobile application. For more information about AppLovin's collection and use of your information visit: https://www.applovin.com/privacy/".

2.3   User shall, in its use or receipt of the Services, Process Personal Data in accordance with the requirements of the Data Protection Laws and User will ensure that its instructions for the Processing of Personal Data comply with the Data Protection Laws. User shall ensure that it has received valid consent and obtained other lawful bases for Processing from Data Subjects as required by Data Protection Laws and, upon AppLovin's request, will provide AppLovin with written evidence of such consent and other lawful bases, including without limitation, the date of the consent and the consent language presented to the Data Subject. User shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which User obtained the Personal Data.

2.4   During the term of the Agreement, AppLovin shall only Process Personal Data in accordance with the Agreement and User's instructions. User instructs AppLovin to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement; and (ii) Processing to comply with other reasonable instructions provided by User where such instructions are consistent with the terms of the Agreement.

2.5   The subject matter of the Processing is the performance of the Services and the Processing shall be carried out for the duration of the Agreement. The types of Personal Data and categories of Data Subjects Processed under this DPA may include the following:

- Types of Personal Data:

  - (a) Mobile device advertising identifiers (e.g., IDFA/Google Ad ID, IP address) and (b) business contact and billing information (e.g., name, email address, billing address, telephone number, VAT number, bank account number).

- Categories of Data Subjects:

  - (a) Individuals who are end-users of User's mobile application(s) and (b) Individuals who are employees, agents or representatives of User in AppLovin's online platform.

3. **RIGHTS OF DATA SUBJECTS**

3.1   To the extent User, in its use or receipt of the Services, does not have the ability to correct, amend, restrict, block or delete Personal Data, as required by Data Protection Laws, AppLovin will use commercially reasonable efforts to comply with reasonable requests by User to facilitate such actions to the extent AppLovin is legally permitted to do so.

3.2   AppLovin shall, to the extent legally permitted, promptly notify User if it receives a request from a Data Subject for access to, correction, amendment, deletion of or objection to the Processing of that Data Subject's Personal Data. AppLovin shall not respond to any such Data Subject request without User's prior written consent except to confirm that the request relates to User. AppLovin shall provide User with commercially reasonable cooperation and assistance in relation to the handling of a Data Subject's request, to the extent legally permitted and to the extent User does not have access to such Personal Data through its use or receipt of the Services.

4.   **PROCESSOR PERSONNEL**

4.1   AppLovin shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and are subject to obligations of confidentiality.

4.2   AppLovin shall ensure that access to Personal Data is limited to those personnel who require such access to perform the Services.

4.3   AppLovin will appoint a data protection officer where such appointment is required by Data Protection Laws.

5.   **SUB-PROCESSORS**

5.1   User acknowledges and agrees that (i) AppLovin Affiliates may be retained as Sub-processors; and (ii) AppLovin may engage third-party Sub-processors in connection with the Services. Any such Sub-processors will be permitted to obtain Personal Data only to deliver the services AppLovin has retained them to provide, and are prohibited from using Personal Data for any other purpose. AppLovin agrees that any agreement with a Sub-processor will include substantially the same data protection obligations as set out in this DPA.

5.2   AppLovin may continue to use those Sub-processors already engaged by AppLovin or any AppLovin Affiliate as at the date of this DPA.

5.3   Where required by Data Protection Laws, AppLovin shall give User notice of the appointment of any new Sub-processor via AppLovin's platform, via email or as otherwise generally made available to AppLovin's advertisers and publishers, including applicable details of the Processing to be undertaken by the Sub-processor. If, within 10 days of receipt of that notice, User notifies AppLovin in writing of any objections (on reasonable grounds) to the proposed appointment, AppLovin shall not appoint that proposed Sub-processor until reasonable steps have been taken to address the objections raised by the User and the User has been provided with a reasonable written explanation of the steps taken.

6.   **SECURITY; AUDIT RIGHTS; PRIVACY IMPACT ASSESSMENTS**

6.1   AppLovin shall maintain administrative, physical and technical safeguards designed to protect the security, confidentiality and integrity of Personal Data.

6.2   No more than once per year, User may engage a mutually agreed upon third-party to audit AppLovin solely for the purposes of meeting its audit requirements pursuant to the Data Protection Laws. To request an audit, User must submit a detailed audit plan at least four (4) weeks in advance of the proposed audit date describing the proposed scope, duration, and start date of the audit. Audit requests must be sent to legal@applovin.com with a copy to dataprotection@applovin.com. The audit must be conducted during regular business hours, subject to obligations of confidentiality and AppLovin's policies, and may not unreasonably interfere with AppLovin's business activities. Any audits are at the User's expense.

6.3   Any request for AppLovin to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those required by law. User shall reimburse AppLovin for any time spent for any such audit at the rates agreed to by the Parties. Before the commencement of any such audit, User and AppLovin shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which User shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by AppLovin. User shall promptly notify AppLovin with information regarding any non-compliance discovered during the course of an audit.

6.4   Where required by Data Protection Laws, AppLovin will reasonably cooperate with User, at User's expense, where User is conducting a data protection impact assessment.

7. **SECURITY BREACH MANAGEMENT AND NOTIFICATION**

7.1   If AppLovin is acting as a Data Processor and becomes aware of any unlawful access to any Personal Data stored on AppLovin's equipment or in AppLovin's facilities, or unauthorized access to such equipment or facilities resulting in material loss, disclosure, or alteration of Personal Data ("Security Breach"), AppLovin will promptly: (i) notify User of the Security Breach; (ii) investigate the Security Breach and provide User with information about the Security Breach; and (iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach.

7.2   User agrees that an unsuccessful Security Breach attempt will not be subject to this Section. An unsuccessful Security Breach attempt is one that results in no unauthorized access to Personal Data or to any of AppLovin's equipment or facilities storing Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, or similar incidents.

7.3   Notification(s) of Security Breaches, if any, will be delivered to one or more of User's business, technical or administrative contacts by any means AppLovin selects, including via email. It is User's sole responsibility to ensure it maintains accurate contact information on AppLovin's support systems at all times.

8. **RETURN AND DELETION OF PERSONAL DATA**

AppLovin shall return Personal Data to User, to the extent possible, and/or delete Personal Data in accordance with AppLovin's data retention policies which adhere to requirements of Data Protection Laws, and in a manner consistent with the terms of the Agreement.

9. **DATA TRANSFERS**

All transfers of Personal Data out of the EEA, the UK and Switzerland to provide the Services shall be governed by the Standard Contractual Clauses attached to this DPA as Attachment A. In addition, AppLovin is certified to and complies with Privacy Shield, and AppLovin shall maintain its certification to and compliance with the Privacy Shield with respect to the Processing of Personal Data that is transferred from the EEA, the UK and Switzerland to the United States.

10. **LIMITATION OF LIABILITY**

Each Party's and all of its Affiliates liability in the aggregate arising out of or relating to this DPA, whether in contract, tort, or under any other theory of liability is subject to the "Limitation of Liability" section of the Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Agreement and all DPAs together.

11. **PARTIES TO THIS DPA**

Except as otherwise expressly set forth in this DPA, nothing in this DPA shall confer any benefits or rights on any person or entity other than the Parties to this DPA.

12. **TERMINATION**

This DPA shall terminate automatically upon termination of the Agreement.

Attachment A

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

User (the "**data exporter**")

and

AppLovin Corporation (the "**data importer**")
Address: 1100 Page Mill Road, Palo Alto, CA 94304 USA
E-mail: dataprotection@applovin.com

each a "**party**"; together "**the parties**",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a)   'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b)   'the data exporter' means the controller who transfers the personal data;

(c)   'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d)   'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e)   'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f)   'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1.   The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2.   The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.   The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have

factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4.   The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a)   that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b)   that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c)   that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d)   that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e)   that it will ensure compliance with the security measures;

(f)   that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g)   to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h)   to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i)   that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j)   that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a)   to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b)   that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c)   that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d)   that it will promptly notify the data exporter about:

(i)   any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii)   any accidental or unauthorised access, and

(iii)   any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e)   to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f)   at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g)   to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h)   that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i)   that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j)   to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3.   The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

<div align="center">**APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES**</div>

Data exporter

User

Data importer

AppLovin Corporation

Data subjects

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

- Individuals who are end-users of data exporter's mobile application(s).

- Individuals who are employees, agents or representatives of data exporter in data importer's online platform.

Categories of data

The personal data transferred concern the following categories of data:

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

- Business contact and billing information (e.g., name, email address, billing address, telephone number, VAT number, bank account number).

Special categories of data

None.

Purpose of Processing

The personal data is processed for the purpose of providing the Services in accordance with the Agreement.

<u>APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES</u>

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Data importer will implement and maintain appropriate administrative, physical, and technical safeguards for the protection of the security, confidentiality and integrity of Personal Data uploaded to the Services.
Those measures shall be set forth in an AppLovin security policy. Data importer will make that policy available to data exporter, along with other information reasonably requested by data exporter regarding data importer's security practices and policies.

CCPA Addendum to AppLovin Data Processing Agreement

This CCPA Addendum ("**CCPA Addendum**") supplements the AppLovin Data Processing Agreement ("**DPA**") and is incorporated into and is subject to the AppLovin Terms of Use Agreement available at https://www.applovin.com/terms (the "**Agreement**") entered into by and between User and AppLovin. This Addendum reflects the parties' agreement in connection with personal information subject to the California Consumer Privacy Act of 2018 ("**CCPA**") and shall be effective solely to the extent CCPA applies. The terms "**consumer**", "**personal information**", "**sale**" and "**service provider**" as used in this CCPA Addendum have the meanings given in the CCPA. Any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement and DPA. If there is any conflict between the terms of this CCPA Addendum and the remainder of the Agreement (including the DPA), the terms of this Addendum will govern.

User and AppLovin agree as follows:

1. AppLovin will act as User's service provider, and as such, will not sell, retain, use or disclose personal information disclosed by User other than (a) on behalf of User for the specific purpose of performing the Services or (b) as may be otherwise permitted for service providers under the CCPA.
2. User will provide all notices and disclosures to its end-users that personal information is being collected and shared for the Services as required by CCPA.
3. This Addendum will be effective as of the later of January 1, 2020 or the date on which User clicked to accept the Agreement or the parties otherwise agreed to the Agreement.