Data Processing Addendum

This Data Processing Addendum ("DPA") forms an integral part of the AppsFlyer Terms of Use, available at https://www.appsflyer.com/terms-of-use/, the master service agreement or similar agreement (including any exhibits, appendices, annexes, terms, orders or policies referenced therein) ("Agreement"), entered into by and between Customer and AppsFlyer that governs Customer’s use and AppsFlyer’s provision of AppsFlyer’s Services. Customer and AppsFlyer are hereinafter jointly referred to as the “Parties” and individually as the “Party”. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

Instructions

This Data Protection Addendum has been pre-signed on behalf of AppsFlyer. To complete this Addendum, please fill in your details and sign in the relevant signature blocks and send the completed and signed DPA to AppsFlyer by email to legal-agreements@appsflyer.com.

In all cases where a specific term in an Agreement incorporates the DPA into the Agreement by reference, the DPA shall be deemed executed upon execution of the Agreement and will be legally binding and made an integral part of the Agreement.

1. Definitions. In addition to capitalized terms defined elsewhere in this DPA, the following terms shall have the meanings ascribed to them herein.

1.1. “Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity.

1.2. “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.

1.3. “Controller” means the natural person or entity that determines the purposes and means of the processing of Personal Data or otherwise is in charge of making decisions regarding the processing of Personal Data.

1.4. "Data Protection Laws" means the data protection or privacy laws in the European Union ("EU"), European Economic Area ("EEA") and their Member States, including the GDPR as well as other similar applicable worldwide data protection laws that relate to the protection of Personal Data.

1.5. “Data Subject” means the identified or identifiable person to whom Personal Data relates.


1.7. “Member States” means a member of the EU.

1.8. “Personal Data” means any information that relates to an identified or identifiable natural person and is protected under Data Protection Laws.

1.9. "Processing" means any operation or set of operations performed upon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.10. “Processor” means a natural person or entity which processes personal data on behalf of the Controller.

1.11. "Standard Contractual Clauses" means the contractual clauses established by the European Commission concerning the international transfer of Personal Data, as set out in Annex 2.
1.12. "Sub Processor" means any Processor appointed by or on behalf of AppsFlyer or any AppsFlyer Affiliate to Process Personal Data on behalf of the Customer in connection with the Agreement; and

1.13. "Supervisory Authority" shall have the same meaning as in the GDPR.

2. Processing of Customer Personal Data.

2.1. The Parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller and AppsFlyer is the Processor. AppsFlyer shall not Process Customer Personal Data other than on the Customer’s documented reasonable and customary instructions, as specified in the Agreement or this DPA, unless such Processing is required by applicable laws to which AppsFlyer is subject.

2.2. Customer instructs AppsFlyer (and authorizes AppsFlyer to instruct each Sub Processor) to (i) Process Customer Personal Data in a manner consistent with the terms of the Agreement and this DPA; and (ii) transfer Customer Personal Data to any country or territory specified in the Agreement or if no such country or territory are specified then to any territory or country, all as reasonably necessary for the provision of the Services and consistent with the Agreement and Section 11 of this DPA.

2.3. Customer warrants and represents that its instructions to Process Personal Data shall at all times comply with Data Protection Laws. Customer shall be solely responsible for the legality of the Personal Data and for ensuring it has an appropriate lawful basis to enable the collection and Processing of Personal Data pursuant to the terms of the Agreement and this DPA.

2.4. Annex 1 sets forth the details of the Processing of Customer Personal Data. In no event shall Customer configure the Services to collect or cause AppsFlyer to Process Personal Data that is beyond the scope set forth in Annex 1, including, specifically any Restricted Data (as defined in the Agreement or if undefined then shall mean any Personal Data beyond the scope of the Personal Data specified in Annex 1).

3. AppsFlyer Personnel. AppsFlyer shall take reasonable steps to ensure that access to the Customer Personal Data is limited on a need to know/access basis and that all AppsFlyer personnel receiving such access are subject to confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access/use of Customer’s Personal Data.

4. Security. AppsFlyer shall, in relation to the Customer Personal Data, implement appropriate technical and organizational measures to ensure an appropriate level of security, including, as appropriate and applicable, the measures referred to in Article 32(1) of the GDPR. In assessing the appropriate level of security, AppsFlyer shall take into account the risks that are presented by Processing PersonData, in particular risks arising from a Personal Data Breach.

5. Sub Processing.

5.1. Customer authorizes AppsFlyer and each AppsFlyer Affiliate to appoint (and permit each Sub Processor appointed in accordance with this Section 5 to appoint) Sub Processors in accordance with this Section 5 and any restrictions in the Agreement.

5.2. The Sub Processors used by AppsFlyer are specified at: https://www.appsflyer.com/subprocessors (“Sub Processors Website”).

5.3. AppsFlyer may appoint new Sub Processors at any time and shall update the Sub Processors Website upon such appointments. If Customer wishes to receive notice of any new Sub Processors, it may request to receive such notice by subscribing at the Sub Processors Website. If, within ten (10) days of such notice, Customer notifies AppsFlyer in writing of any reasonable objections to the proposed appointment, AppsFlyer shall not utilize such Sub Processor to Process Customer Personal Data until reasonable steps have been taken to address the objections raised by Customer, and Customer has been provided with a reasonable written explanation of the steps taken. Where such steps are not sufficient to relieve Customer’s reasonable objections then Customer or AppsFlyer may, by written notice
to the other Party, with immediate effect, terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub Processor, without bearing liability for such termination.

5.4. With respect to each Sub Processor, AppsFlyer shall: (a) take reasonable steps to ensure that the Sub Processor is committed to provide the level of protection for Personal Data required by the Agreement; (b) ensure that the arrangement between AppsFlyer and the Sub Processor is governed by a written contract, including terms which, to the extent applicable to the nature of services provided by the Sub Processor, offer a level of protection that, in all material respects, are consistent with the levels set out in this DPA and the Agreement; and (c) remain fully liable to the Customer for the performance of the Sub Processor’s data protection obligations where the Sub Processor fails to fulfill such obligations.

6. **Data Subject Rights.**

6.1. Customer shall be solely responsible for compliance with any statutory obligations concerning requests to exercise Data Subject rights under Data Protection Laws (e.g. for access, rectification or deletion of Customer Personal Data etc.). Taking into account the nature of the Processing, AppsFlyer shall reasonably assist Customer insofar as feasible, to fulfil Customer’s said obligations with respect to such Data Subject requests, as applicable, at Customer’s sole expense.

6.2. AppsFlyer: (a) shall promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data (unless prohibited by applicable law); and (b) shall not respond to that request except on the documented instructions of Customer or as required by applicable laws. Notwithstanding the foregoing, AppsFlyer shall be permitted to respond (including through automated responses) to any such requests informing the Data Subject that his request has been received and/or with instructions to contact Customer in the event that his request relates to Customer.

7. **Personal Data Breach.**

7.1. AppsFlyer shall notify Customer, without undue delay, upon AppsFlyer becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise processed by AppsFlyer (“Personal Data Breach”). In such event, AppsFlyer shall provide Customer with information (to the extent in AppsFlyer’s possession) to assist Customer to meet any obligations to inform Data Subjects or Data Protection authorities of the Personal Data Breach under the Data Protection Laws.

7.2. At the written request of the Customer, AppsFlyer shall reasonably cooperate with Customer and take such commercially reasonable steps, as are agreed by the Parties or necessary under Data Protection Laws, to assist in the investigation, mitigation and remediation of each such Personal Data Breach, at Customer’s sole expense.

8. **Data Protection Impact Assessment and Prior Consultation.**

8.1. At the written request of the Customer, AppsFlyer and each AppsFlyer Affiliate shall provide reasonable assistance to Customer, at Customer's expense, with any data protection impact assessments or prior consultations with Supervising Authorities or other competent data privacy authorities, as required under any applicable Data Protection Laws. Such assistance shall be solely in relation to Processing of Customer Personal Data by AppsFlyer.

9. **Deletion or return of Customer Personal Data.**

9.1. AppsFlyer shall return or make available to Customer the Personal Data per the terms of the Agreement, or if no such terms are provided then immediately prior to termination of the Agreement. Following termination of the Agreement, Personal Data shall be deleted or otherwise made unrecoverable and/or anonymized, other than such copies, as authorized under the Agreement or this DPA, or required, to be retained in accordance with applicable law and/or regulation.

10. **Audit Rights**
10.1. Subject to sections 10.2 and 10.3, AppsFlyer shall make available to Customer on request such information necessary to demonstrate compliance with this DPA and shall allow for, and contribute to, audits by a reputable auditor mandated by Customer in relation to the Processing of the Customer Personal Data by AppsFlyer.

10.2. To the extent AppsFlyer has undergone a third party independent audit based on SOC 2, Type II or similar standards, then any audit right arising pursuant to section 10.1 shall be first satisfied by providing Customer with a report of such audit. If Customer, for reasonable reasons, is not satisfied by the independent audit report then Customer may request that a reputable auditor perform an audit pursuant to section 10.1 and subject to Section 10.3. If AppsFlyer does not agree to such additional audit or inspection, then Customer shall have the right to terminate the Agreement with immediate effect.

10.3. Customer shall give AppsFlyer reasonable prior written notice of any audit or inspection to be conducted under Section 10.1 and shall use (and ensure that each of its mandated auditors uses) its best efforts to avoid causing any damage, injury or disruption to AppsFlyer’s premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. All such audits shall be subject to the confidentiality obligations set forth in the Agreement. Customer and AppsFlyer shall mutually agree upon the scope, timing and duration of the audit or inspection in addition to any reimbursement of expenses for which Customer shall be responsible. Any such audits shall not occur more than once a year (except where required by law or due to a Personal Data Breach). Additionally, AppsFlyer need not give access to its premises for the purposes of such an audit or inspection: (a) to any individual unless he or she produces reasonable evidence of identity and authority; (b) to any competitor of AppsFlyer; or (c) outside AppsFlyer’s normal business hours.

11. **Transfers** Customer acknowledges that AppsFlyer may transfer and Process Personal Data outside of the country from which it originated in order to perform the services for Customer including to such countries identified on the Sub Processors Website. Customer shall ensure it obtains any necessary consents or has the necessary rights to enable such transfer. Subject to the foregoing, AppsFlyer shall only make such transfers in compliance with Data Protection Laws and in particular with respect to any transfers of Personal Data under the Agreement from the EU, EEA, Member States and Switzerland to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws or which transfer is not otherwise governed by a framework approved by the European Commission to which AppsFlyer is officially certified, shall be subject to the Standard Contractual Clauses. The Standard Contractual Clauses shall come into effect and be deemed executed upon execution of this DPA and shall apply pursuant to the order of precedence described in the preceding sentence.

12. **General Terms**

12.1. **Agreement and Order of Precedence.** Nothing in this DPA reduces either Party’s obligations under the Agreement in relation to the collection, use, processing and protection of Personal Data. Any claims brought under this DPA shall be subject to the terms of the Agreement including, without limitation, choice of jurisdiction, governing law and any liability limitations or exclusions. In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Agreement and including (except where explicitly agreed otherwise in writing and signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

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

[**SIGNATURE PAGE FOLLOWS**]
IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the later date set out below.

**Customer.**

Company Name: ____________

Signature: ________________

Name: ________________

Title: ________________

Date: ________________

**AppsFlyer Ltd.**

Signature: [Signature]

Name: Oren Kaniel

Title: CEO

Date: September 26, 2021

**AppsFlyer Inc.**

Signature: [Signature]

Name: Oren Kaniel

Title: CEO

Date: September 26, 2021
Annex 1: Details Of Processing Of Customer Personal Data

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

**Subject matter and duration of the Processing of Customer Personal Data.** The subject matter of the Processing of the Customer Personal Data is to provide attribution and analytics services, as are further described in the Agreement. The duration shall be for the period set forth in the Agreement.

**The nature and purpose of the Processing of Customer Personal Data:** rendering Services in the nature of an attribution and marketing analytics platform, as further detailed in the Agreement.

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

The data types that may be processed when using the services:

- **“Technical Information”:** this refers to technical information related to an End User’s mobile device or computer, such as: browser type, device type and model, CPU, system language, memory, OS version, Wi-Fi status, time stamp and zone, device motion parameters and carrier.

- **"Technical Identifiers":** this refers to various unique identifiers that generally only identify a computer, device, browser or Application. For example, IP address (which may also provide general location information), User agent, IDFA (identifier for advertisers), Android ID (in Android devices); Google Advertiser ID, Customer issued user ID and other similar unique identifiers.

- **"Engagement Information":** this refers to information relating to the Customer’s ad campaigns and End User actions, such as: clicks on Customer ads, ad impressions viewed, audiences or segments to which an ad campaign is attributed, the type of ads and the webpage or Application from which such ads were displayed, the webpages on Customer’s website visited by an End User, the URL from the referring website, downloads and installations of Applications, and other interactions, events and actions Customers choose to measure and analyze within their Application or website (e.g. add to cart, in-app purchases made, clicks, engagement time etc.).

- Any other data types explicitly agreed by the Parties under the Agreement.

For the purpose of clarity, Customer shall not configure the Services to collect any data that is not permitted to be collected pursuant to the terms of the Agreement or that is beyond the scope identified above.

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

End users who use or interact with Customer's websites, products, services, advertisements and mobile application services.
STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A (hereinafter each ‘data exporter’), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each ‘data importer’)

have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

Clause 8.1(b), 8.9(a), (c), (d) and (e);

Clause 9(a), (c), (d) and (e);

Clause 12(a), (d) and (f);

Clause 13;

Clause 15.1(c), (d) and (e);

Clause 16(e);

Clause 18(a) and (b).

Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES
Clause 8
Data protection safeguards
The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions
(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation
The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency
On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy
If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data
Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify
the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural
person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter ‘sensitive data’), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (\(^2\)) (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.
Clause 9

Use of sub-processors

(a) The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (f) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter’s request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor’s obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party(ies) for any damages it causes the other Party(ies) by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

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.

[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.

[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.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that
laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination— including those requiring the disclosure of data to public authorities or authorising access by such authorities — relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (\(^4\));

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal
data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the country where customer is incorporated as set out in the main agreement between Parties.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the country where customer is incorporated as set out in the main agreement between Parties.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.
APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.
A. LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: _the entity defined as Customer in the DPA_______________

Address: _________________________________________

Contact person’s name, position and contact details: _________________________
___________________________________________________________________

Activities relevant to the data transferred under these Clauses:
___________________________________________________________________
___________________________________________________________________

Signature and date: ___________________________________________________

Role (controller):

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: _AppsFlyer Ltd.__________________________

Address: ______14 Maskit st. Herziliya, Israel _________

Contact person’s name, position and contact details: _privacy@appsflyer.com_____________________

___________________________________________________________________

Activities relevant to the data transferred under these Clauses:
_________N/A_________________________________________

___________________________________________________________________

Signature and date: ___________________________________________________

Role processor):
B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As described in Annex 1 to the DPA.

Categories of personal data transferred

As described in Annex 1 to the DPA.

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.

It is not intended that AppsFlyer receive any special categories of data.

...

Nature of the processing

As described in Annex 1 to the DPA.

Purpose(s) of the data transfer and further processing

As described in Annex 1 to the DPA...

...

...

C. COMPETENT SUPERVISORY AUTHORITY

The Supervisory Authority of the Member State in which Data Exporter is located
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Access Controls: Administrative access to our production environment is limited to a restricted number of individuals. Access to additional individuals is given only in extreme circumstances, for a specific purpose, and is limited in duration. Such access to these additional individuals is given only after the explicit approval of the security team. User access is based upon termination and evaluated on a quarterly basis.

Physical and Environmental Security: General access to the office is controlled by the use of a card access system. Cameras are installed throughout the sites. Access to controlled areas is restricted through the use of card access and/or additional verification. All individuals without authorized access to the controlled areas must sign in and be escorted by an individual with approved controlled area access.

Application Security: AppsFlyer has developed and implemented a strict, secure development program, based on Open Web Application Security Project (OWASP), and Microsoft Security Development Lifecycle. From the earliest phases of product design and planning, the security team takes an active role in how our products are built. Following completion, sensitive product developments are tested to ensure that application security has been thoroughly and properly addressed.

Vulnerability monitoring through penetration testing: Data importer performs at least two annual Information Security penetration tests, which are conducted by accredited and completely independent information security companies. Vulnerabilities, if found, are addressed as part of our Risk Management Policy. AppsFlyer performs vulnerability assessment scanning using third-party tools at least twice a month, and after any major infrastructure change in our production environment.

Data transfer security: Data transferred to data importer through its services are encrypted in transit by default on all supporting browsers. In addition, data recorded on HTTPS pages is fully encrypted and transferred to servers over a TLS connection.

Networks security: AppsFlyer implements multiple and varied infrastructure security measures to protect customer information from unauthorized access, loss, alteration, viruses, Trojans and other similar harmful code. This includes: Swift and regular updates of operating systems, hardware, and any third party software to avoid security vulnerabilities. Critical updates are deployed within one week from release on corporate as well as production systems. Use of firewalls and Intrusion Prevention Systems (IPS) systems to limit access and protect AppsFlyer servers. Hardening of all external-facing servers according to industry best practices. Implementing anti-malware controls to prevent entry of malicious software. Securing remote access communication using multifactor authentication. Backing up customer data on a daily basis, on a rotating schedule.
Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.