Data Processing Agreement

in accordance with Art. 28 GDPR

between

Advertiser

hereinafter referred to as the "**Controller**"

and

AppLift GmbH

10178 Berlin

Germany

hereinafter referred to as the "**Processor**"

Preamble

The Controller has selected the Processor to act as a service provider in accordance with Art. 28 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, "**GDPR**").

This Data Processing Agreement, including all Annexes (hereinafter referred to collectively as the "**Agreement**"), specifies the data protection obligations of the parties from the underlying Advertiser Terms and Conditions and/or the order descriptions

(hereinafter referred to collectively as the "**Principal Agreement**"). If reference is made to the regulations of the Federal Data Protection Act (hereinafter referred to as "**FDPA**"), this refers to the German Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680, as amended on 25 May 2018. If reference is made to the regulations of the German Federal Data Protection Act-old ("**FDPA-old**"), this refers to the German Federal Data Protection Act as amended in the announcement dated 14 January 2003 (BGBl. I p. 66).

The Processor guarantees the Controller that it will fulfil the Principal Agreement and this Agreement in accordance with the following terms:

Sect. 1 Scope and definitions

(1) The following provisions shall apply to all services of data processing provided by the Processor on behalf of the Controller under Art. 28 GDPR, which the Processor performs on the basis of the Principal Agreement, including all activities which may involve the processing of personal data by the Processor on behalf of the Controller.

(2) If this Agreement uses the term "data processing" or "processing" of data, this shall be generally understood to mean the use of personal data. Data processing or the processing of data shall mean any operation or set of operations which is performed on personal data or on 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.

(3)Reference is made to further definitions set forth in Art. 4 GDPR.

Sect. 2 Subject matter and duration of the data processing

(1) The Processor shall process personal data on behalf and in accordance with the instructions of the Controller.

(2) The data processing shall involve making available to the Controller certain end user tracking features to assist Controller with generation, selection and optimization of end users' targeting decisions as well as the provision of a platform for the placement of targeted advertisements in mobile advertising inventory as agreed upon in the Principal Agreement.

(3) The duration of this Agreement corresponds to the duration of the Principal Agreement.

Sect. 3 Nature and purpose of the data processing

The nature and purpose of the processing of personal data by the Processor is specified in the Principal Agreement. The Principal Agreement includes the following activities and purposes:

- Performance of online marketing campaigns for Controller's mobile app as per Controller's instructions (e.g. targeting and retargeting of specific audiences)

Sect. 4 Categories of data subjects

The categories of individuals affected by the processing of personal data under this Agreement (“data subjects”) include:

- App Users
    - Existing users
    - Potential (new) users
- Controller employees (permanent staff, trainees, temporary workers, freelancers)
- Controller (external) supply partners

Sect. 5 Types of personal data

The following types of personal data shall be processed under this Agreement:

Consumer personal data:

- Electronic communications data (e.g. IP address, device ID, advertising ID, web/app content accessed, information on the terminal device, operating system and browser used)
    - Business partner data
- External user login information consisting of:
- Email address
- Name
- Job Title

Sect. 6 Rights and duties of the Controller

(1) The Controller is solely responsible for assessing the lawfulness of the data processing and for safeguarding the rights of data subjects, and is hence a controller within the meaning of Art. 4 (7) GDPR.

(2) The Controller is entitled to issue instructions concerning the nature, scale and method of data processing. Upon request by the Controller, the Processor shall confirm verbal instructions immediately in writing or in text form (e.g. by email).

(3) Insofar as the Controller deems it necessary, persons authorized to issue instructions may be appointed. The Processor shall be notified of such in writing or in text form. In the event that the persons authorized to issue instructions change, the Controller shall notify the Processor of this change in writing or in text form, naming the new person in each case.

(4) The Controller shall notify the Processor immediately of any errors or irregularities detected in relation to the processing of personal data by the Processor.

(5) If the Controller is obliged to designate a representative under Art. 27 (1) GDPR, the Controller will inform the Processor of the name and the contact data of its representative via e-mail to dataprotection@applift.com within two weeks after the conclusion of this Agreement. The representative shall be instructed to act as a contact point in addition to the Controller or in its place, in particular for supervisory authorities

and data subjects, for all questions related to processing in order to ensure compliance with data protection regulations.

(6) If the Controller is obliged to designate a Data Protection Officer under Art. 37 (1) GDPR, the Controller will inform the Processor of the name and the contact data of its representative via e-mail to dataprotection@applift.com within two weeks after the conclusion of this Agreement.

Sect. 7 Duties of the Processor

(1) Data processing

The Processor shall process personal data in accordance with this Agreement and/or the underlying Principal Agreement and in accordance with the Controller's instructions. The Processor shall also process the personal data for fraud prevention, bot detection, ad security, ad verification services and service misuse prevention.

(2) Data subjects' rights

a. The Processor shall, within its capabilities, assist the Controller in complying with the rights of data subjects, particularly with respect to rectification, restriction of processing, deletion of data, notification and information. If the Processor processes the personal data specified under Sect. 5 of this Agreement on behalf of the Controller and these data are the subject of a data portability request under Art. 20 GDPR, the Processor shall, upon request, make the dataset in question available to the Controller within the

set time frame, otherwise within seven business days, in a structured, commonly used and machine-readable format.

b. If so instructed by the Controller, the Processor shall rectify, delete or restrict the processing of personal data specified under Sect. 5 of this Agreement. The same applies if this Agreement stipulates the rectification, deletion or restriction of the processing of data.

c. If a data subject contacts the Processor directly to have his or her data specified under Sect. 5 of this Agreement rectified, deleted or the processing restricted, the Processor shall forward this request to the Controller immediately upon receipt.

(3) Monitoring duties

a. The Processor shall ensure, by means of appropriate controls, that the personal data processed on behalf of the Controller are processed solely in accordance with this Agreement and/or the Principal Agreement and/or the relevant instructions.

b. The Processor shall organize its business and operations in such way that the data processed on behalf of the Controller are secured to the extent necessary in each case and protected from unauthorized access by third parties.

c. The Processor confirms that it has appointed a Data Protection Officer in accordance with Art. 37 GDPR and in accordance with Sect. 38 FDPA, and that the Processor shall monitor compliance with data protection and security laws.

(4) Information duties

a. The Processor shall inform the Controller immediately if, in its opinion, an instruction issued by the Controller violates legal regulations. In such cases, the Processor shall be entitled to suspend execution of the relevant instruction until it is confirmed or changed by the Controller.

b. The Processor shall assist the Controller in complying with the obligations set out in Articles 32 to 36 GDPR to within its capabilities.

(5) Location of processing

Any transfer of personal data outside the European Union or the European Economic Area may only take place if the special requirements of Art. 44 et seqq. GDPR are fulfilled.

(6) Deletion of personal data after order completion

After termination of the Principal Agreement, the Processor shall hand over to the Controller all personal data, documents and work results that are associated with the contractual relationship or delete or destroy them in accordance with data protection law after prior consent of the Controller, provided that the deletion of these data does not conflict with any statutory storage obligations of the Processor. The deletion in accordance with data protection and data security regulations must be documented and confirmed upon request in writing or text form to the Controller.

Sect. 8 Monitoring rights of the Controller

(1) The Controller shall be entitled, after prior notification in good time and during normal business hours, to carry out an inspection of compliance with the provisions on data protection and the contractual agreements to the extent required, either himself or through third parties, without disrupting the Processor's business operations or endangering the security measures for other Controller and at his own expense. Controls can also be carried out by accessing existing industry-standard certifications of the Processor, current attestations or reports from an independent body (such as auditors, external data protection officers or external data protection auditors) or self-assessments. The Processor shall offer the necessary support to carry out the checks.

(2) The Processor shall inform the Controller of the execution of inspection measures by the supervisory authority to the extent that such measures or requests may concern data processing operations carried out by the Processor on behalf of the Controller.

Sect. 9 Subprocessing

(1) The Controller authorizes the Processor to make use of other processors in accordance with the following subsections in Sect. 9 of this Agreement. This authorization shall constitute a general written authorization within the meaning of Art. 28 (2) GDPR.

(2) The Processor currently works with the subcontractors specified in **Annex 2** and the Controller hereby agrees to their appointment.

(3) The Processor shall be entitled to appoint or replace other processors. The Processor shall inform the Controller in advance of any intended change regarding the appointment or replacement of another processor. The Controller may object to an intended change.

(4) The objection to the intended change must be lodged with the Processor within 2 weeks after receipt of the information on the change. In the event of an objection, the Processor may, at its own discretion, provide the service without the intended modification or – if the provision of the service is unreasonable for the Processor without the intended modification – terminate this Agreement and the Principal Agreement without notice.

(5) A level of protection comparable to that of this Agreement must always be guaranteed when another processor is involved. The Processor is liable to the Controller for all acts and omissions of other processors it appoints.

Sect. 10 Confidentiality

(1) The Processor is obliged to maintain confidentiality when processing data for the Controller.

(2) In fulfilling its obligations under this Agreement, the Processor undertakes to employ only employees or other agents who are committed to confidentiality in the handling of personal data provided and who have been appropriately familiarized with the

requirements of data protection. Upon request, the Processor shall provide the Controller with evidence of the confidentiality commitments.

(3) Insofar as the Controller is subject to other confidentiality provisions, it shall inform the Processor accordingly. The Processor shall oblige its employees to observe these confidentiality rules in accordance with the requirements of the Controller.

Sect. 11 Technical and organizational measures

(1) The technical and organizational measures described in **Annex 1** are agreed upon as appropriate. The Processor may update and amend these measures provided that the level of protection is not significantly reduced by such updates and/or changes.

(2) The Processor shall observe the principles of due and proper data processing in accordance with Art. 32 in conjunction with Art. 5 (1) GDPR. It guarantees the contractually agreed and legally prescribed data security measures. It will take all necessary measures to safeguard the data and the security of the processing, in particular taking into account the state of the art, as well as to reduce possible adverse consequences for the affected parties. Measures to be taken include, in particular, measures to protect the confidentiality, integrity, availability and resilience of systems and measures to ensure continuity of processing after incidents. In order to ensure an appropriate level of processing security at all times, the Processor will regularly evaluate the measures implemented and make any necessary adjustments.

Sect. 14 Miscellaneous

(1) In case of contradictions between the provisions contained in this Agreement and provisions contained in the Principal Agreement, the provisions of this Agreement shall prevail.

(2) Amendments and supplements to these provisions must be in writing or in text form and expressly declare that the provisions in this Agreement are being changed and/or supplemented. The foregoing also applies to the formal requirement itself.

(3) This Agreement is exclusively subject to the laws of the Federal Republic of Germany.

(4) Before 25 May 2018, this Agreement shall constitute a Data Processing Agreement within the meaning of Sect. 11 FDPA-old. The provisions of the FDPA-old shall apply accordingly until 25 May 2018.

(5) In the event that access to the data which the Controller has transmitted to the Processor for data processing is jeopardized by third-party measures (measures taken by an insolvency administrator, seizure by revenue authorities, etc.), the Processor shall notify the Controller of such without undue delay.

(6) The plea of a right of retention pursuant to Sect. 273 German Civil Code (*Bürgerliches Gesetzbuch, BGB*) with respect to the processed data and the associated storage medium is precluded.

_____

Place, date

_____

Signature (Controller)

_____

Place, date

_____

Signature (Processor)

Schedule of Annexes

Annex 1 Technical and organizational measures taken by the Processor to ensure the security of processing

Annex 2 Subprocessors pursuant to Sect. 9 of this Data Processing Agreement

Annex 1

Technical and organizational measures to ensure the security of processing

The Processor guarantees that the following technical and organizational measures have been taken:

A. Encryption measures

Measures or operations in which a clearly legible text/information is converted into an illegible, i.e. not easily interpreted, character string (secret text) by means of an encryption method (cryptosystem).

Description of the encryption measure(s):

• *Use of HTTPS (which uses block algorithms internally) to encrypt communication between the user's browser and AppLift servers, and between AppLift and ad exchanges (if they support it)*

• *Use of encryption for communication across certain data centers*

B. Measures to ensure confidentiality

1. Physical access control

Measures that physically deny unauthorized persons access to IT systems and data processing equipment used to process personal data, as well as to confidential files and data storage media.

Description of physical access control:

• *ID card reader for electronically controlled key assignment, i.e. chip card*

• *Door protection (electronic door opener, fingerprint access control)*

• *Factory security/gatekeeper (for certain offices)*

• *Alarm systems and video surveillance*

• *Control system for visitors: visitor check in system with photo & name*

2. Logical access control

Measures to prevent unauthorized persons from processing or using data which is protected by data privacy laws.

Description of logical access control system:

• *Password procedure, i.e. personal and individual login user credentials when logging on to the system (e.g. special characters, minimum length, regular password change)*

• *Limitation of the number of authorized employees*

• *Encryption of data carriers*

• *Access lists*

• *Authentication procedures*

• *Logging of authentication attempts and aborting the logon process after a specific number of unsuccessful attempts*

• *Regularly updated antivirus and spyware filters*

• *Offboarding processes to prevent leavers from having access to company data*

• *Limiting access to production servers to employees – access is only provided for short*

amounts of time on an as needed basis and requires management approvals

• *Leveraging security features of third parties (Google) extensively such as 2 phase authentication and SSO, and leveraging other third-party services (e.g. namely) that utilize Google's SSO*

3. Data access control

Measures to ensure that persons authorized to use data processing systems can only access personal data according to their access rights, so that data cannot be read, copied, changed or removed without authorization during processing, use and storage.

Description of data access control:

• *Role-based access control in AWS and GCP*

• *Tight control over data access in SoftLayer. No production server access to anyone other than the operational team responsible for managing servers (DevOps), other than as an exception*

• *Automated deployment of code from source code repositories to production servers*

• *Use of HTTPS in communication between the user's browser and AL servers*

• *Access to data through the product restricts access based on roles and scope.*

4. Separation rule

Measures to ensure that data collected for different purposes are processed separately and separated from other data and systems in such a way as to preclude the unplanned use of such data for other purposes.

Description of the separation control process:

• *Authorization concepts*

• *Architectural separation of different systems and data processing units on different hosts with different access lists*

• *Separation of test and production systems*

D. Measures to ensure integrity

1. Data integrity

Measures to ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system.

Description of data integrity:

• *Import of new releases and patches with release/patch management*

• *Functional test during installation and releases/patches by the IT department*

• *Audit of database changes with rollback capability*

• *Automated backups with the ability to restore past versions*

2. Transmission control

Measures to ensure that it is possible to verify and establish to which bodies personal data may be or have been transmitted or made available using data communication equipment.

Description of transmission control:

• *Transport processes with individual responsibility*

• *Authentication and authorization around data shared with partners via API's*

3. Transport control

Measures to ensure that the confidentiality and integrity of data is protected during transmission of personal data and transport of data carriers.

Description of transport control:

• *Transmission of data via encrypted data networks or tunnel connections (VPN)*

• *Encryption methods that detect data changes during transport*

• *Use of dedicated links in communication between datacenters when they belong to the same vendor*

• *Use of HTTPS (whenever possible) in communication between datacenters when they belong to different vendors*

• *Use of VPN's in office to datacentre communication*

• *Special validation logic for data files coming from partners*

4. Input control

Measures to ensure that it can be subsequently verified and ascertained whether and by whom personal data have been entered or modified in data processing systems.

Description of the input control process:

• *Use of partner identity tokens such as APIKEY in validating source of write API requests*

• *Recording of user requests to fetch partner data from static sources such as file or URL*

E. Measures to ensure availability and resilience

1. Availability control

Measures to ensure that personal data are protected against accidental destruction or loss.

Description of the availability control system:

• *Data backup procedure*

• *Use of high availability infrastructure provided by subprocessors*

• *Uninterrupted power supply*

• *Fire alarm system*

• *Alarm system*

2. Quick recovery

Measures to ensure the ability to quickly restore the availability of and access to personal data and used systems in the event of a physical or technical incident.

Description of the measures for quick recovery:

• *Recovery procedures of subprocessors*

• *Regular tests of data recovery*

3. Reliability

Measures to ensure that the functions of the system are available and malfunctions are reported.

Description of measures for reliability:

• *Automatic monitoring with email and instant messaging*

• *Hot issue escalation and reporting processes*

F. Measure for the regular testing and evaluation of the security of data processing

1. Verification process

Measures to ensure that the data are processed securely and in compliance with data protection regulations.

Description of verification process:

• *Documentation of instructions received by the Controller*

• *Formalized order management*

• *Automated code deployments*

2. Order control

Measures to ensure that personal data processed on behalf of the Controller can only be processed in accordance with the instructions of the Controller.

Description of the order control measures:

• *Controller instructions recorded through changelog features in the software*

Annex 2

Subprocessors pursuant to Sect. 9 Data Processing Agreement

The Processor currently works with the following subcontractors and the Controller hereby agrees to their appointment.

Company: Everflow Technologies Inc.

Data processing activity: Marketing platform software

Location [city, country]: San Francisco, California, USA

Contact information: privacy@everflow.io

Company: Amazon Web Services, Inc

Data processing activity: Cloud storage provider

Location [city, country]: 12th Avenue South Suite, 1200 Seattle, WA 98144, USA

Contact information: privacyshield@amazon.com

Company: Google

Data processing activity: Cloud services and physical storage provider, presynching of user device IDs for targeting on google ad exchange

Location [city, country]: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Contact information: support-de@google.com