

## Data Protection Addendum

This Data Protection Agreement addendum ("DPA") form an integral part of the service agreement between: (i) Mobfolio acting as "Controller" and (ii) Publisher acting as "Processor"

The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect. In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below related to General Data Protection Regulation 2016/679 is the Principal Agreement. Except where the context requires otherwise.

"GDPR" means EU General Data Protection Regulation 2016/679;

"Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Controller, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

"Agreement" means either the Mobfolio T&C or Mobfolio Service Agreement (as applicable) and the related DPA, which together govern the provision of the Services to Controller.

"Controller Data" means any Personal Data that Publisher processes on behalf of Controller as a Data Processor in the course of providing Services.

"Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country

"EEA" means the European Economic Area;

"Data Controller" means an entity that determines the purposes and means of the processing of Personal Data.

"Data Processor" means an entity that processes Personal Data on behalf of a Data Controller.

"EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

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

"Processing" has the meaning given to it in the GDPR and "process", "processes", and "processed" will be interpreted accordingly.

“Security Incident” means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Controller Data.

“Services” means any product or service provided by Publisher to Controller pursuant to the Agreement.

“Sub-processor” means any Data Processor engaged by Publisher or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA.

Relationship with the Agreement.

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”).

The parties agree that this DPA will replace any existing data protection addendum or similar agreement the parties may have previously entered into in connection with the Services.

Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA will prevail to the extent of that conflict. Any claims brought under or in connection with this DPA will be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

Any claims against Publisher or its Affiliates under this DPA will be brought solely against the entity that is a party to the Agreement. Controller further agrees that any regulatory penalties or other liability incurred by Publisher in relation to the Controller Data that arise as a result of, or in connection with, Controller’s failure to comply with its obligations under this DPA or any applicable Data Protection Laws will count toward and reduce Publisher’s liability under the Agreement as if it were liability to the Controller under the Agreement.

No one other than a party to this DPA, its successors and permitted assignees will have any right to enforce any of its terms.

This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws. Scope and Applicability of this DPA.

This DPA applies where and only to the extent that Publisher processes Controller Data that originates from the EEA and/or that is otherwise subject to EU Data Protection Law on behalf of Controller as Data Processor in the course of providing Services pursuant to the Agreement.

Role of the Parties. As between Publisher and Controller, Controller is the Data Controller of Controller Data, and Publisher will process Controller Data only as a Data Processor acting on behalf of Controller.

Controller Processing of Controller Data. Controller agrees that: (i) it will comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Controller Data and any processing instructions it issues to Publisher ; and (ii) it has provided notice and obtained all consents and rights necessary under Data Protection Laws for Publisher to process Controller Data and provide the Services pursuant to the Agreement and this DPA.

Publisher Processing of Controller Data. Publisher will process Controller Data only for the purposes described in the DPA accordance with Controller's documented lawful instructions and the EU General Data Protection Regulation 2016/679. The parties agree that this DPA and the GDPR instructions are the Agreement set out the Controller's complete and final instructions to Publisher in relation to the processing of Controller Data and processing outside the scope of these instructions (if any) will require prior written agreement between Controller and Publisher .

The purpose of the data processing under this DPA is the provision of the Services to the Controller and the performance of Publisher pursuant to the Agreement (including this DPA) or as otherwise agreed by the parties.

Subject matter and duration of the data processing

The Processor shall process personal data on behalf and in accordance with the instructions of the Controller and the "GDPR" guidelines. 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.

The duration of this Agreement corresponds to the duration of the Principal Agreement.

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: Online marketing campaigns for Controller's mobile app/s as per Controller's instructions.

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 users, Controller employees, Controller (external) supply partners

Legitimate Interests. Notwithstanding anything to the contrary in the Agreement (including this DPA), Controller acknowledges that Publisher will have a right to use and disclose data relating to the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered Personal Data under Data Protection Laws and “GDPR” guidelines, Publisher is the Data Controller of such data and accordingly will process such data in accordance with the Publisher Privacy Policy and Data Protection Laws of “GDPR”.

Tracking Technologies. Controller acknowledges that in connection with the performance of the Services, Publisher employs the use of cookies, unique identifiers, web beacons and similar tracking technologies (“Tracking Technologies”). Controller will maintain appropriate notice, consent, opt-in and opt-out mechanisms as are required by Data Protection Laws to enable Publisher to deploy Tracking Technologies lawfully on, and collect data from, the devices of Recipients in accordance.

#### Personal Data

Processor will collect and process only non-sensitive data signals. Personal data will be pseudonymized and encrypted to maintain the privacy of the user. The data will be processed for standard advertising use cases: campaign operations; performance attribution and optimization; brand targeting; brand measurement and will comply with “GDPR” guidelines.

#### Subprocessing.

Authorized Sub-processors. Controller agrees that Publisher may engage Sub-processors to process Controller Data on Controller’s behalf.

Sub-processor Obligations. Publisher will: (i) enter into a signed agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Controller Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Publisher to breach any of its obligations under this DPA.

#### Security.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Controller Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

Publisher is responsible for reviewing the information made available by Controller relating to data security and making an independent determination as to whether the Services meet

Controller's requirements and legal obligations under Data Protection Laws. Controller acknowledges that the Security Policy is subject to technical progress and development and that Publisher may update or modify the Security Policy from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Controller.

Controller Responsibilities. Notwithstanding the above, Controller agrees that except to the extent expressly provided in this DPA, Controller is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Controller Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Controller Data uploaded to the Services.

Confidentiality of Processing. Publisher will ensure that any person who is authorized by Publisher to process Controller Data (including its staff, agents and subcontractors) will be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

Security Incident Response.

Processor shall notify Controller without any delay upon Processor or any Sub-processor becoming aware of a Personal Data Breach affecting Controller Personal Data, providing Company with sufficient information to allow Controller to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

Audits.

Upon request, Publisher will supply a summary copy of its audit report(s) ("Report") to Controller, so that Controller can verify Publisher's compliance with the audit standards against which it has been assessed, and this DPA. Such Reports, as well as any conclusions or findings specified therein, are Publisher's Confidential Information.

Publisher will also provide written responses to all reasonable requests for information made by Controller, including responses to information security and audit questionnaires that are necessary to confirm Publisher's compliance with this DPA, provided that Controller will not exercise this right more than once per year. Such responses are Publisher's Confidential Information.

International Transfers.

Processing Locations. Publisher may transfer and process Controller Data anywhere in the world where Publisher, its Affiliates or its Sub-processors maintain data processing operations. Publisher will at all times provide an adequate level of protection for the Controller Data processed, in accordance with the requirements of Data Protection Laws and "GDPR" guidelines.

Privacy Shield. To the extent that Publisher processes any Controller Data protected by EU Data Protection Law under the Agreement and/or that originates from the EEA, in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority

(as applicable) as providing an adequate level of protection for Personal Data, the parties acknowledge that Publisher will be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Controller Data by virtue of having self-certified its compliance with Privacy Shield. Publisher agrees to protect such Personal Data in accordance with the requirements of the Privacy Shield Principles. If Publisher is unable to comply with this requirement, Publisher will inform Controller.

**Alternative Transfer Mechanism.** The parties agree that the data export will not apply if and to the extent Publisher adopts an alternative data export solution for the lawful transfer of Personal Data (as recognized under EU Data Protection Laws) outside of the EEA (“Alternative Transfer Mechanism”), in which event, the Alternative Transfer Mechanism will apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which Personal Data is transferred).

#### **Return or Deletion of Data.**

Upon termination or expiration of the Agreement, Publisher will (at Controller’s election) delete or return to Controller all Controller Data (including copies) in its possession or control, save that this requirement will not apply to the extent Publisher is required by applicable law to retain some or all of the Controller Data, or to Controller Data it has archived on back-up systems, which Controller Data Publisher will securely isolate and protect from any further processing, except to the extent required by applicable law.

#### **Cooperation.**

**Data Subject Requests.** The Services provide Controller with a number of controls that Controller may use to retrieve, correct, delete, or restrict Controller Data, which Controller may use to assist it in connection with its obligations under the GDPR including, for example, its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent Controller is unable to independently access the relevant Controller Data within the Services, Publisher will provide reasonable cooperation to assist Controller to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event any such request is made directly to Publisher, Publisher will not respond to such communication directly without Controller’s prior authorization, unless legally compelled to do so.

If Publisher is required to respond to such a request, Publisher will promptly notify Controller and provide it with a copy of the request unless legally prohibited from doing so.

**Records of Processing.** Upon request from Controller, Publisher will make available in a timely manner such information as is required by Controller to demonstrate Publisher’s compliance with its obligations under EU Data Protection Law and under this DPA.

**Government Requests.** If a law enforcement agency sends Publisher a demand for Controller Data such as by court order, Publisher will attempt to redirect the law enforcement agency to request that data directly from Controller. As part of this effort, Publisher may provide Controller’s basic contact information to the law enforcement agency. If compelled to disclose

Controller Data to a law enforcement agency, then Publisher will give Controller reasonable notice of the demand to allow Controller to seek a protective order or other appropriate remedy unless Publisher is legally prohibited from doing so.

Data Protection Impact Assessments. To the extent Publisher is required under EU Data Protection Law, Publisher will (at Controller's expense to the extent legally permitted) provide reasonably requested information regarding the Services to enable the Controller to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

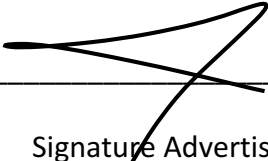
Updated: May 24th, 2018

**May24th 2018**

---

Place, date

---



Signature Advertiser (Controller)

---

Place, date

---

Signature (Processor)