

DATA PROTECTION ADDENDUM

1. SCOPE

- a. Mobknow or its Affiliate, as identified in the Agreement ("**Company**") and Partner (each "**Party**"), as defined below, are parties to the Agreement, as defined below, to which this Data Protection Addendum applies.
- b. If Partner Processes Personal Data, or if Partner has access to Personal Data in the course of its performance under the Agreement, Partner shall comply with the terms and conditions of this Data Protection Addendum ("**Data Protection Addendum**"). By signing this Data Protection Addendum, Partner shall qualify as the Data Processor, as this term is defined under Data Protection Laws. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

2. DEFINITIONS

All capitalized terms not defined in this Data Protection Addendum have the meanings set forth in the Agreement.

- a. "**Affiliate**" means any person or entity directly or indirectly controlling, controlled by, or under common control with a Party. For the purpose of this definition, "control" (including, with correlative meanings, the terms "controlling", "controlled by" and "under common control with") means the power to manage or direct the affairs of the person or entity in question, whether by ownership of voting securities, by contract or otherwise.
- b. "**Agreement**" means the agreement between Company and Partner which involves Partner having access to or otherwise Processing Personal Data;
- c. "**Approved Jurisdiction**" means a member state of the EEA, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here:
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.
- d. "**Breach Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- e. "**Data Protection Laws**" means any and/or all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state or deferral or national level, pertaining to data privacy, data security and/or the protection of Personal Data, including the Data Protection Directive 95/46/EC and the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), including any amendments or replacements to them, including the 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 ("**GDPR**").
- f. "**EEA**" means those countries that are member of the European Economic Area.
- g. "**Partner**" refers to the legal entity, regardless of the form of organization, identified in the Agreement.
- h. "**Personal Data**" or "**personal data**" has the meaning as defined in the Data Protection Laws.
- i. "**Process**" or "**process**" has the meaning as defined in the Data Protection Laws. "**Processes**" or "**processes**" and "**Processing**" or "**processing**" shall be construed accordingly.
- j. "**Special Categories of Data**" has the meaning as defined in the Data Protection Laws.

3. DATA PROTECTION AND PRIVACY

- a. If Partner has access to or otherwise Processes Personal Data, then Partner shall:
 - i. only Process the Personal Data for the duration of the Agreement in accordance with Company's documented instructions and on its behalf, and in accordance with the Agreement and this Data Protection Addendum;
 - ii. take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process, Personal Data; ensure persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and ensure that such personnel are aware of their responsibilities under this Data Protection Addendum and any Data Protection Laws (or Partner's own written binding policies are at least as restrictive as this Data Protection Addendum);
 - iii. assist Company as needed to cooperate with and respond to requests from supervisor authorities, data subjects, customers, or others to provide information (including details of the services provided by Partner) related to Partner's Processing of Personal Data;
 - iv. notify the Company without undue delay, and no later than twenty four (24) hours, after becoming aware of a Breach Incident;
 - v. provide full, reasonable cooperation and assistance to Company in:
 - a. allowing data subjects to exercise their rights under the Data Protection Laws, including (without limitation) the right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or the right not to be subject to an automated individual decision making;

- b. ensuring compliance with any notification obligations of personal data breach to the supervisory authority and communication obligations to data subjects, as required under Data Protection Laws;
- c. Ensuring compliance with its obligation to carry out data protection impact assessments with respect to the Processing of Personal Data, and with its prior consultation with the supervisory authority obligation (as applicable).
- vi. only process or use Personal Data on its systems or facilities to the extent necessary to perform its obligations under the Agreement;
- vii. as required under Data Protection Laws, maintain accurate written records of any and all the Processing activities of any Personal Data carried out under the Agreement (including the categories of Processing carried out and, where applicable, the transfers of Personal Data), and shall make such records available to the applicable supervisory authority on request;
- viii. make all reasonable efforts to ensure that Personal Data are accurate and up to date at all times while in its custody or under its control, to the extent Partner has the ability to do so;
- ix. not lease, sell or otherwise distribute Personal Data;
- x. promptly notify Company of any investigation, litigation, arbitrated matter or other dispute relating to Partner's information security or privacy practices as it relates to the Processing of Personal Data;
- xi. promptly notify Company in writing and provide Company an opportunity to intervene in any judicial or administrative process if Partner is required by law, court order, warrant, subpoena, or other legal or judicial process to disclose any Personal Data to any person other than Company;
- xii. upon termination of the Agreement, or upon Company's written request at any time during the term of the Agreement, Partner shall cease to Process any Personal Data received from Company, and within a reasonable period will at the request of Company: (1) return the Personal Data; or 2) securely and completely destroy or erase all Personal Data in its possession or control (including any copies thereof), unless and solely to the extent the foregoing conflicts with any applicable laws. At Company's request, Partner shall give Company a certificate confirming that it has fully complied with this clause.

4. SUBCONTRACTING

- a. Partner shall not subcontract its obligations under this Data Protection Addendum to another person or entity ("**Contractor(s)**"), in whole or in part, without Company's prior written approval or general written authorization, and shall inform the Company of any intended changes concerning the addition/replacement of other processors.
- b. Partner will execute a written agreement with such approved Contractor containing equivalent terms to this Data Protection Addendum provided that Partner shall not be entitled to permit the Contractor to further sub-contract or otherwise delegate all or any part of the Contractor's processing without Company's prior written consent at Company's sole discretion) and which expressly provides Company with third party beneficiary rights to enforce such terms and/or require Partner to procure that the Contractor enters into a Data Protection agreement with Company directly.
- c. Partner shall have a written security policy that provides guidance to its Contractors to ensure the security, confidentiality, integrity and availability of Personal Data and systems maintained or processed by Partner.
- d. Company may require Partner to provide Company with full details of the proposed Contractor's involvement including but not limited to the identity of the Contractor, its data security record, the location of its processing facilities and a description of the access to Personal Data proposed.
- e. Partner shall be responsible for the acts or omissions of Contractors to the same extent it is responsible for its own actions or omissions under this Data Protection Addendum.

5. THE TRANSFER OF PERSONAL DATA

- a. If the Partner is required to transfer Personal Data to a third country or an international organization under applicable laws, it shall inform the Company of that legal requirement before processing; If, subject to Company's prior consent, Partner Processes Personal Data from the EEA in a jurisdiction that is not an Approved Jurisdiction, Partner shall ensure that it has a legally approved mechanism in place to allow for the international data transfer.
- b. If Partner intends to rely on Standard Contractual Clauses, the following additional terms will apply to Partner and Partner's partners and/or affiliates (where subcontracting or performance is allowed by the Agreement):
 - i. If the Standard Contractual Clauses are superseded by new or modified Standard Contractual Clauses, the new or modified Standard Contractual Clauses shall be deemed to be incorporated into this Data Protection Addendum, and Partner will promptly begin complying with such Standard Contractual Clauses. Partner will abide by the obligations set forth under the Standard Contractual Clauses for data importer and/or sub-processor as the case may be.
 - ii. If Partner subcontracts any Processing of Personal Data (as allowed by the Agreement and Applicable Law), it will:
 - a. Notify and obtain Company's advance written permission before proceeding; and
 - b. Ensure that it has a legally approved mechanism in place to allow for the international data transfer, or that Contractors have entered into the Standard Contractual Clauses with Partner.

6. SECURITY STANDARDS

- a. Partner shall implement and maintain commercially reasonable and appropriate physical, technical and organizational security measures to protect Personal Data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed; all other unlawful forms of Processing; including (as appropriate): (i) the pseudonymisation and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing
- b. To the extent that Partner Processes Special Categories of Data, the security measures referred to in this Data Protection Addendum shall also include, at a minimum (i) routine risk assessments of Partner’s information security program, (ii) regular testing and monitoring to measure and confirm the effectiveness of the information security program’s key controls, systems, and procedures, and (iii) encryption of Special Categories of Data while “at rest” and during transmission (whether sent by e-mail, fax, or otherwise), and storage (including when stored on mobile devices, such as a portable computer, flash drive, PDA, or cellular telephone).

7. GENERAL

- a. If any of the Data Protection Laws are superseded by new or modified Data Protection Laws (including any decisions or interpretations by a relevant court or governmental authority relating thereto), the new or modified Data Protection Laws shall be deemed to be incorporated into this Data Protection Addendum, and Partner will promptly begin complying with such Data Protection Laws.
- b. Any ambiguity in this Data Protection Addendum shall be resolved to permit Company to comply with all Data Protection Laws. In the event and to the extent that the Data Protection Laws impose stricter obligations on the Partner than under this Data Protection Addendum, the Data Protection Laws shall prevail.
- c. If this Data Protection Addendum does not specifically address a particular data security or privacy standard or obligation, Partner will use appropriate, generally accepted practices to protect the confidentiality, security, privacy, integrity, availability, and accuracy of Personal Data.
- d. Partner agrees that, in the event of a breach of this Data Protection Addendum, neither Company nor any relevant Company's customer will have an adequate remedy in damages and therefore either Company or an affected customer shall be entitled to seek injunctive or equitable relief to immediately cease or prevent the use or disclosure of Personal Data not contemplated by the Agreement and to enforce the terms of this Data Protection Addendum or ensure compliance with all Data Protection Laws.
- e. If Partner is unable to provide the level of protection as required herein, Partner shall immediately notify Company and cease processing. Any non-compliance with the requirements herein shall be deemed a material breach of the Agreement and Company shall have the right to terminate the Agreement immediately without penalty.
- f. Company, shall have the right to: (a) require from Partner all information necessary to, and (b) conduct its own audit and/or inspections of Partner (including its facilities or equipment involved in the Processing of Personal Data) in order to: demonstrate compliance with the Data Protection Addendum. Such audit and/or inspection shall be conducted with reasonable advanced notice to Partner, and shall take place during normal business hours to reasonably limit any disruption to Partner’s business.

IN WITNESS WHEREOF, this Data Protection Addendum has been signed by the Partner:


	Partner	Company
By:	_____	_____
Title:	_____	_____
Date:	_____	25/5/18
Signature:	_____	

EXHIBIT A – DATA SHARING PROTOCOL

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

- end users of the Company's clients or advertising partners
- Affiliates and partners

The transfer is made for the following purposes:

- Providing advertising and app monetization experience
- Customer service activities, such as processing orders, payment processing, technical support and improving offerings
- Consulting, professional, security, storage, hosting and other related services
- Internal business processes and management, age verification or authentication purposes, fraud detection and prevention, and compliance with governmental, legislative and regulatory bodies
- Sales and marketing

The personal data transferred concern the following categories of data:

- Profile data (IP address)
- Other: [complete]