DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**DPA**") forms part of and is subject to the terms of the Agreement (the "**Agreement**") by and between **Mobupps International Ltd** ("**Company**") and you, the contracting Party to the Agreement (**"Supplier")**

1. Subject Matter.

1.1. **Subject Matter.** This DPA reflects the parties' commitment to abide by Data Protection Laws as this term is define below, concerning the Processing of Personal Data as this term is defined below in connection with the execution of the Agreement**.**

1.2. **In case Supplier is an Advertiser**, then Supplier shall act as the data controller under the meaning of the Data Protection Laws and the provisions of this DPA regarding processing shall be interpreted to be applicable to the Supplier as a controller. The Advertiser warrants and represents that it has a lawful basis for any personal data it collects, processes, or uses in connection with this Agreement, including but not limited to for targeting, tracking, or retargeting advertising. The Advertiser is solely responsible for ensuring that all necessary consents have been obtained and that data subjects have been informed in accordance with the Data Protection Laws. Advertiser is solely responsible for managing and responding to data subject's access requests, objections, and complaints. Company acts solely as a data processor, where applicable, and does not determine the purposes or means of processing personal data. Company does not receive, collect, or store any personal data from or on behalf of the Advertiser in the course of delivering advertising services. Any ad-serving, tracking, or analytics functions carried out by the Company do not involve access to or processing of identifiable personal data unless expressly agreed in writing. Any data processed by Company (such as anonymized IP data, browser type, or aggregated campaign statistics) is strictly limited to non-identifiable information and is used solely for service optimization, delivery, or fraud prevention. Such data shall not be considered personal data under the Data Protection Laws.

1.3. **In case Supplier is a Publisher, Ad Network, Agency etc.,** then the parties acknowledge and agree that, with respect to any personal data processed under this agreement, Parties to this agreement are acting solely as a data processor. Nothing in this agreement shall be construed to grant a Party independent rights or responsibilities as a controller of personal data.

1.4. For the purpose of the present Agreement, no personal data shared between the parties, only aggregated data. If upon further analysis the Parties decide that personal data needs to be shared between the parties, the Parties shall act according to this Data Processing Addendum and any the Applicable Data Protection Laws.

1.5. If Supplier collects any Personal Data, Supplier shall be solely responsible for ensuring that all Personal Data remain confidential and that any collection, processing, storage and/or transmission of such Personal Data complies with all applicable rules, regulations and laws, including but not limited to privacy laws. Supplier shall immediately notify Company in writing of any breach or violation hereof. Supplier shall immediately notify Company in writing prior to any transfer of Personal Data to Company if such transfer would violate any rule, regulation or law, and in no event shall Supplier transfer Personal Data unless and until such risk of violation is removed or corrected. Supplier shall implement commercially reasonable technical, administrative and physical procedures to protect Personal Data from unauthorized use, alteration, disclosure, distribution or access.

1.6. This DPA will become legally binding upon the signature date of the Agreement and will continue in effect so long as Supplier Processes Personal Data.

2. Definitions.

2.1. "**Data Protection Laws**" means all applicable data privacy, data protection, and cybersecurity laws, rules and regulations to which the Personal Data are subject. "Data Protection Laws" may include, but are not limited to, the California Consumer Privacy Act of 2018 ("**CCPA**"); the California Privacy Rights Act ("**CPRA**"); the Virginia Consumer Data Protection Act ("**VCDPA**"); the Colorado Privacy Act ("**CPA**"), the Connecticut Data Protection Act ("**CTDPA**"), the Utah Consumer Privacy Act ("**UCPA**") ; Australia's the Privacy Act 1988 ("**APP**") ; Canada's Personal Information Protection and Electronic Documents Act ("**PIPEDA**"); Québec's Act Respecting the Protection of Personal Information in the Private Sector ("**Private Sector Act**"); British Columbia's Personal Information Protection Act ("**BC PIPA**"); Alberta's Personal Information Protection Act ("**AB PIPA**"); the EU General Data Protection Regulation 2016/679 ("**GDPR**") and its respective national implementing legislation; the Swiss Federal Act on Data Protection; the United Kingdom General Data Protection Regulation; and the United Kingdom Data Protection Act 2018("**UK GDPR**") (in each case, as amended, adopted, or superseded from time to time) and other data protection/privacy laws which take effect during the term of the Agreement and any other relevant privacy legislation.

2.2. "**Permitted Purpose(s)**" means the Processing necessary to provide and operate Mobupps' advertising technology and related services, including advertising delivery, RTB and bid processing, campaign management, impression and click measurement, conversion and install attribution, reporting, optimization, fraud prevention, security, billing, troubleshooting and technical support. Types of data collected are, where applicable, inter ilia, IP address; device and advertising identifiers; browser/device information; approximate location; contextual information; impression/click/conversion/install data; consent and privacy signals; campaign identifiers and fraud/security information. Supplier shall not use Personal Data received from or on behalf of Mobupps to create or enrich profiles, audiences, datasets or user segments for its own purposes or for the benefit of another customer, advertiser or third party, except to the extent expressly authorized in writing and permitted under applicable Data Protection Laws.

2.3. "**Personal Data**" has the meaning assigned to the terms "personal data" or "personal information" under applicable Data Protection Laws, and will, at a minimum, mean any information relating to an identified or identifiable natural person.

2.4. "**Process**" or "**Processing**" means any operation or set of operations which is performed on 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.

2.5. "**Security Incident(s)**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

2.6. "**Subprocessor(s)**" means a Supplier's vendors, service providers, and other third parties that Process Personal Data, which Supplier must notify the Company of their existence and details, in advance.

3. Processing.

3.1. Supplier's Role Under Data Protection Laws. Supplier is a separate "Service Provider" and/or "Processor" of Personal Data (as such terms are defined by Data Protection Laws). Under no circumstances shall the parties be considered joint "Controllers" under Data Protection Laws.

3.2. Use of Personal Data. Supplier shall Process Personal Data solely for the Permitted Purpose, and solely to the extent necessary to carry out the Permitted Purpose, in each case, in accordance with the Agreement, this DPA, and Data Protection Laws.

3.3. Transparency. Supplier shall maintain a publicly available privacy notice that clearly and accurately describes its practices with respect to its collection, use, and disclosure of Personal Data. To the extent applicable to the services, Supplier shall support and comply with the IAB Europe Transparency & Consent Framework ("TCF") and its applicable policies and technical requirements. Supplier shall not circumvent, disable or materially interfere with consent signals or other privacy choices transmitted through the TCF or other applicable consent-management mechanisms. Supplier shall Process Personal Data in accordance with the consent signals and applicable purposes and legal bases communicated through such mechanisms, to the extent applicable to Supplier's role and the relevant Processing activity. Supplier shall provide reasonable cooperation to Mobupps in relation to consent signals, privacy choices, and compliance with applicable TCF requirements.

3.4. Additional Processing of Personal Data. If Supplier Processes any other Personal Data in connection with the Agreement (e.g., Personal Data about Company and Supplier customers that Supplier directly collects from such individuals), Supplier shall Process such Personal Data in accordance with applicable laws.

3.5. Supplier and Subprocessor Compliance. Supplier shall (i) enter into a written agreement with Subprocessors regarding such Subprocessors' Processing of Personal Data that imposes on such Subprocessors use restrictions and data protection and information security requirements for Personal Data that is at least as protective as the obligations in this DPA, and requires Subprocessor to enter into similar written contracts with their respective Subprocessors;,; and (iii) remain fully liable to Company for Supplier's Subprocessors' (if applicable) failure to perform their obligations with respect to the Processing of Personal Data.

3.6. Confidentiality. Any person authorized to Process Personal Data must contractually agree to maintain the confidentiality of such information or be under an appropriate statutory obligation of confidentiality.

3.7. Personal Data Inquiries and Requests. Supplier shall, to the extent legally permitted, promptly notify Company if it receives a request from a data subject to exercise an individual right under Data Protection Laws or otherwise, including rights for access to, or correction, amendment, blocking, restriction, or deletion of that data subject's Personal Data, only if such request may impact Company's Processing of Personal Data. Supplier shall

independently, timely, and fully address any data subject's request to exercise rights under Data Protection Law or otherwise.

3.8. Sale of Personal Data Prohibited and CCPA. Supplier shall process Personal Information only for specified business purposes; not sell or share Personal Information as the term "sell" is defined by the CCPA; not retain, use or disclose Personal Information outside the purposes specified in the agreement; not combine the Personal Information with information obtained from another source except as permitted by the CCPA; provide the same level of privacy protection required of a service provider/contractor; notify Mobupps if it can no longer comply; allow Mobupps to take reasonable steps to ensure compliance or permit Mobupps to stop or remediate unauthorized use.

3.9. Data Protection Impact Assessment and Prior Consultation. Supplier agrees to provide reasonable assistance to Company where, in Company's judgement, the type of Processing performed in connection with the Agreement requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

3.10. Children's Data / COPPA. Supplier shall not knowingly collect, use, disclose or otherwise Process Personal Data relating to children under 13 in connection with the services in a manner that would violate the Children's Online Privacy Protection Act ("COPPA") or applicable implementing regulations. Supplier shall comply with applicable requirements concerning children's data and shall promptly notify Mobupps if it becomes aware that it has received or Processed Personal Data relating to a child in circumstances not authorized under the Agreement or applicable law. In addition, Supplier shall not use children's Personal Data for targeted advertising or behavioral advertising where prohibited by applicable law.

3.11. Demonstrable Compliance. Supplier agrees to provide information reasonably necessary to demonstrate compliance with this DPA upon Company's reasonable request.

4. Information Security.

4.1. Information Security Program. Supplier shall maintain and implement a documented information security program designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data. Such program shall be risk-based and shall take into account the nature, scope, context and purposes of the Processing and the risks to the rights and freedoms of individuals. Supplier shall regularly review and, where appropriate, update its security measures and procedures.

4.2. Security Policies and Procedures. Supplier shall maintain appropriate written information security, privacy, incident response, business continuity and data protection policies and procedures. Such policies and procedures shall be periodically reviewed and updated and communicated to personnel with relevant responsibilities.

4.3. Personnel Security and Confidentiality. Supplier shall ensure that personnel authorized to Process Personal Data are subject to appropriate confidentiality obligations and receive appropriate privacy and information-security training. Where legally permitted and appropriate to the nature of the role and access involved, Supplier shall implement personnel screening procedures for personnel authorized to access Personal Data.

4.4. Access Controls. Supplier shall implement role-based access controls and the principles of least privilege and need-to-know. Access to Personal Data and systems Processing Personal Data shall be limited to personnel who require such access to perform their assigned functions. Supplier shall maintain procedures for the granting, modification and prompt revocation of access rights, including upon termination of employment or a change in role.

4.5. Authentication and Privileged Access. Supplier shall maintain appropriate authentication and credential-management controls. Multi-factor authentication shall be implemented for privileged accounts and, where appropriate based on risk, for accounts providing access to Personal Data or production systems. Shared user credentials shall not be permitted for access to systems Processing Personal Data, except where technically unavoidable and subject to appropriate compensating controls.

4.6. Network and System Security. Supplier shall maintain appropriate technical controls designed to prevent unauthorized access to systems and Personal Data, including, as appropriate, network segregation, secure system configurations, access controls, endpoint security and other measures appropriate to the nature and risks of the Processing. Where Supplier operates a multi-tenant environment, Supplier shall maintain logical segregation and access controls designed to prevent unauthorized access to Personal Data belonging to one customer or tenant by another.

4.7. Encryption and Secure Transmission. Supplier shall implement encryption and other appropriate measures to protect Personal Data in transit and at rest, taking into account the nature and sensitivity of the Personal Data and the risks associated with the Processing. Personal Data transmitted over public or otherwise untrusted networks

shall be protected using industry-standard secure communication protocols. Backups containing Personal Data shall be appropriately protected, including through encryption where appropriate.

4.8. Vulnerability Management. Supplier shall maintain a vulnerability management program appropriate to its systems and services, including monitoring for known vulnerabilities, security updates and patches, risk-based remediation and appropriate security testing. Supplier shall address identified vulnerabilities within timeframes appropriate to their severity and the associated risks.

4.9. Penetration Testing and Security Assessments. Supplier shall periodically assess the effectiveness of its security controls and, where appropriate having regard to the nature and risks of the Processing, conduct vulnerability assessments and penetration testing of systems that Process Personal Data. Supplier shall remediate material findings identified through such assessments within a reasonable period appropriate to the severity of the finding.

4.10. Secure Software Development. Where Supplier develops, maintains or materially modifies software used to Process Personal Data, Supplier shall maintain a secure software development lifecycle appropriate to the services and risks involved. Such practices shall include, where appropriate, security considerations during design, risk assessment, code review, vulnerability testing, change management and controlled deployment.

4.11. Logging and Monitoring. Supplier shall maintain appropriate logging and monitoring mechanisms for systems Processing Personal Data, including, where appropriate, authentication events, privileged access, access to Personal Data, security events and relevant system activity. Supplier shall monitor relevant systems for anomalous or unauthorized activity and shall maintain procedures for investigating and responding to identified security events.

4.12. Security Incident Management. Supplier shall maintain documented procedures for the detection, escalation, investigation, containment, mitigation, remediation and recovery of Security Incidents. Supplier shall document material Security Incidents and the measures taken in response and shall conduct appropriate post-incident reviews to identify and address measures necessary to prevent recurrence. More details are provided in Section 5 herein.

4.13. Business Continuity and Disaster Recovery. Supplier shall maintain business continuity and disaster recovery procedures appropriate to the nature and risks of the Processing. Such procedures shall include appropriate backup, restoration and recovery measures designed to enable the timely restoration of the availability and access to Personal Data following a physical or technical incident. Backups shall be appropriately protected and shall be tested periodically to verify their integrity and recoverability.

4.14. Availability and Resilience. Supplier shall maintain reasonable measures designed to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services used to Process Personal Data, taking into account the nature and risks of the Processing.

4.15. Data Segregation. Where Personal Data is Processed in systems or environments shared with other customers or third parties, Supplier shall maintain appropriate logical and technical controls designed to segregate Mobupps' Personal Data from data belonging to other customers or third parties and to prevent unauthorized cross-customer access.

4.16. Data Deletion. Supplier shall maintain procedures for the secure deletion or destruction of Personal Data when it is no longer required for the purposes for which it was Processed, upon expiry or termination of the applicable services, or pursuant to Mobupps' documented instructions, subject to applicable legal retention requirements. Personal Data contained in routine backups may be deleted in accordance with Supplier's ordinary backup-retention cycle, provided that such data remains protected and is not restored or otherwise Processed except as necessary for legitimate backup, disaster-recovery or legal purposes.

4.17. Regular Review and Testing. Supplier shall regularly test, assess and evaluate the effectiveness of its technical and organizational security measures and shall implement improvements where reasonably necessary to address identified risks or material changes in the Processing environment.

4.18. Evidence of Compliance. Upon reasonable request, Supplier shall provide Mobupps with information reasonably necessary to demonstrate its compliance with this Section 4, including relevant security policies, certifications, audit reports, penetration-test summaries or other appropriate evidence, subject to confidentiality and security restrictions.

5. Security Incidents.

5.1. Security Incident Procedure. Supplier will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to reasonably suspected or

known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Personal Data in a timely manner.

5.2. Notice. Supplier agrees to provide written notice without undue delay (but in no event longer than twenty-four (24) hours) to Company's Designated POC if it knows or reasonably suspects that a Security Incident has taken place. Such notice will include all reasonably available details relevant to the Security Incident. Company may request additional information related to the Security Incident following Supplier's notice and Supplier shall provide such information within a reasonable period of time.

~~5.3.~~ Remediation. Supplier shall: (i) investigate, remediate and take any other action Company deems necessary regarding the Security Incident; (ii) provide full cooperation and assistance to Company in connection with any dispute, inquiry, investigation, claim, or order concerning the Security Incident; and (iii) provide Company with assurance satisfactory to Company that such Security Incident will not recur. Supplier will be fully liable for all costs and expenses incurred by Supplier and/or Company in connection with the Security Incident.

6. Cross-Border Transfers of Personal Data.

6.1. Cross-Border Transfers of Personal Data. To the extent necessary under the Agreement, Company authorizes Supplier to transfer Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States, provided that such transfer complies with Data Protection Laws. If Supplier, its Subprocessors Process Personal Data originating in the European Economic Area, Switzerland, and/or United Kingdom in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws, the parties agree that the applicable laws and regulations shall also apply.

6.2. Standard Contractual Clauses - To the extent Supplier or its Subprocessors process Personal Data originating from the European Economic Area ("EEA"), Switzerland, or the United Kingdom in a country that has not been recognized as providing an adequate level of protection under applicable Data Protection Laws, the Parties agree that the transfer shall be governed by the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as set out in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("SCCs"), which are hereby incorporated into this DPA by reference. The Parties agree that: Processor to Processor (Module Three) shall apply, as relevant to the role of the Parties under this DPA. The details required by Annex I, II, and III of the SCCs shall be deemed completed with the information set forth in this DPA (including the definitions, security measures, processing details, and subprocessors listed herein). For transfers subject to the UK GDPR, the SCCs shall apply together with the UK International Data Transfer Addendum (IDTA) issued by the UK Information Commissioner's Office ("ICO"), as incorporated by reference. For transfers subject to the Swiss Federal Act on Data Protection, the SCCs shall apply with the modifications required by the Swiss Federal Data Protection and Information Commissioner (FDPIC).

7. Records.

7.1. Records, Supplier shall maintain a record of processing activities in accordance with the Data Protection Laws. This record shall include details of the categories of processing, the nature and purpose of the processing, categories of data subjects and personal data involved, any transfers of personal data outside the relevant jurisdiction, and a description of the technical and organizational measures used to protect such data. Supplier shall make such records available to Company or to any competent supervisory authority upon request

7.2. Company Audit. Company (or its appointed representative) may carry out an audit of Supplier's premises, architecture, systems, policies, procedures, and records relevant to the Processing of Personal Data. Any audit must be: (i) conducted during Supplier's regular business hours; (ii) with reasonable advance notice to Supplier; (iii) carried out in a manner that prevents unnecessary disruption to Supplier's operations; and (iv) subject to reasonable confidentiality procedures. Following an audit, Supplier shall make any necessary changes to ensure compliance with its obligations under this DPA at its own expense and without unreasonable delay and shall notify Company when such changes are complete.

8. Storage and Deletion.

8.1. Data Storage. Supplier will not store or retain any Personal Data except as necessary to carry out the Permitted Purposes or as required by applicable laws.

8.2. Data Deletion. Upon Company's request, Supplier will securely destroy all copies of Personal Data (including automatically created archival copies) and certify said action in writing.

9. Indemnification.

9.1. Indemnity. Supplier shall indemnify, defend, and hold harmless Company and its officers, directors, employees and agents from and against any claims, disputes, demands, liabilities, damages, losses, fines, and costs and expenses, including, without limitation, reasonable attorneys' fees arising out of or relating to a Security Incident.

10. Miscellaneous.

10.1. Disputes and Claims. In the event of an inquiry, dispute, or claim brought by a data subject concerning Supplier's Processing of Personal Data, Supplier will inform Company about any such inquiry, dispute, or claim, and will cooperate with Company with a view to resolving such issues within a reasonable time.

10.2. Remediation of Processing. Upon notice from Company, Supplier shall immediately remediate any Processing that Company reasonably believes violates an applicable privacy policy, notice, or similar document or impacts Company's Processing of such Personal Data, or Company's compliance with Data Protection Laws.

10.3. Laws and Jurisdiction In the event of a dispute regarding this DPA, the laws and jurisdiction clause of the Agreement shall govern this DPA.

10.4. Company and Supplier agree to designate a point of contact for urgent privacy and security issues (a "**Designated POC**"). The Designated POC for both parties are:

For Company:

Email: contact@mobupps.com

Telephone: +972 8 622 9900

Address: Tikshoret 7, Ashdod, Israel 77700

For Supplier: _____

Company	**Supplier**
Signature: _____	Signature: _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
Email: _____	Email: _____