DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") forms part of the terms of service, as updated from time to time, found at https://www.crowdfireapp.com/tos, or other agreement between Customer and Crowdfire and its affiliates governing Customer's use of the service ("**Agreement**").

This Addendum regulates the Processing of Personal Data subject to EU Data Protection Law for the Purposes (as defined in Section 3) by the Parties in the context of the service. The terms used in this Addendum have the meaning set forth in this Addendum. Except as modified below, the Agreement remains in full force and effect. Annex 1 forms an integral part of this Addendum.

This Addendum has been pre-signed on behalf of Crowdfire. To complete this DPA, Customer must sign on page 3 and send the signed Addendum to Crowdfire by email.

The Parties agree that the terms and conditions set out below are added as an Addendum to the Agreement.

1. **Definitions.** The following terms have the meanings set out below for this Addendum:

1.1. "Controller" means the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

1.2. "Data Subject" means a natural person located in the EEA whose Personal Data is processed in the context of this Addendum.

1.3. "EU Data Protection Law" means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) and their national implementing legislations; the Swiss Federal Data Protection Act (as amended and replaced from time to time); and the Data Protection Acts of the EEA countries (as amended and replaced from time to time).

1.4. "Europe" means the European Economic Area ("**EEA**") and Switzerland.

1.5. "Personal Data" means any information relating to an identified or identifiable natural person who is a Data Subject. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

1.6. "Personal Data Breach" 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.

1.7. "Processor" means the entity which processes Personal Data on behalf of a Controller.

1.8. "Processing of Personal Data" (or "Processing/Process") means 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.

1.9. "Standard Contractual Clauses" means the clauses annexed to EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010, p. 5-18) but excluding the optional ind

1.10. "Sub-Processor" means the entity engaged by the Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Controller.

2. **Roles of the Parties.** For the purposes of this Addendum, the Parties acknowledge and confirm that Customer is a Controller and Crowdfire is a Processor for the Processing of Personal Data for the Purposes (as defined in Section 3) in the context of the service.

3. **Description of the Processing Activities.** Crowdfire will Process Personal Data to provide its Services as described in the Terms of Service and only for the purpose of providing such Services, in particular publishing your content on social platforms ("Purposes"). A full list of personal information that we may collect is outlined in our Privacy Policy.

4. **Obligations of Customer.** Customer confirms and warrants that, in relation to the Processing of Personal Data for the Purposes in the context of the Service, it acts as a Controller and that: (a) it complies with EU Data Protection Law when Processing Personal Data, and only gives lawful instructions to Crowdfire; (b) Data Subjects have been informed of the uses of Personal Data as required by EU Data Protection Law; (c) it ensures there is a valid legal ground for the processing of Personal Data under EU Data Protection Law (d) it complies with Data Subject requests to exercise their rights of access, rectification, erasure, data portability, restriction of Processing, and objection to the Processing, and rights relating to automated decision-making; (e) it complies with data accuracy, proportionality and data retention principles; (f) implements appropriate technical and organizational measures to ensure, and to be able to demonstrate, that the Processing of Personal Data is performed in accordance with EU Data Protection Law; and (g) it will cooperate with Crowdfire to fulfill their respective data protection compliance obligations in accordance with EU Data Protection Law.

5. **Obligations of Crowdfire.** Crowdfire confirms and warrants that it complies with EU Data Protection Law when Processing Personal Data for the Purposes in connection with the Service, and that it:

5.1. Only Processes Personal Data on behalf of the Customer in accordance with the use and performance of the service and not for any other purposes than those specified in Section 3 or as otherwise agreed by both Parties in writing. For the avoidance of doubt, Customer authorizes Crowdfire to de- identify Personal Data for Crowdfire's product development, product improvement, benchmarking and analytics purposes.

5.2. Will promptly inform Customer if, in its opinion, Customer's instructions infringe EU Data Protection Law, or if Crowdfire is unable to comply with Customers' instructions. Crowdfire shall inform Customer of any applicable legal requirement under EU or EU member state law that prevents Crowdfire from complying with Customer's instructions, unless that law prohibits such information on important grounds of public interest.

5.3. Will notify Customer without undue delay after becoming aware of a Personal Data Breach. Crowdfire will take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach.

5.4. Will assist Customer in complying with data security, data breach notifications, data protection impact assessments, and prior consultations with supervisory authorities requirements under EU Data Protection Law, taking into account the nature of the Processing and the information available to Crowdfire. To the extent authorized under applicable law, Customer shall be responsible for any costs arising from Crowdfire's provision of such assistance.

5.5. Taking into account the nature of the processing, will assist Customer by appropriate technical and organizational measures, insofar as this is possible, to fulfill Customer's obligation to respond to Data Subjects' requests to exercise their rights as provided under EU Data Protection Law and specified in Clause 4. To the extent authorized by applicable, Customer shall be responsible for any costs arising from Crowdfire's provision of such assistance.

6. **Data Transfers.**

6.1. To provide the Service, Crowdfire needs to import Personal Data to the United States and India. Customer authorizes such cross-border Personal Data transfers and confirms and warrants that it will comply with any requirements under EU Data Protection Law with regard to such Personal Data transfers.

6.2. By signing this Addendum, the Parties execute the Standard Contractual Clauses. The Standard Contractual Clauses are hereby incorporated into this Addendum, and completed as follows: (a) Customer is the "data exporter", (b) Crowdfire is the "data importer", (c) the applicable law in Section 10 of this Addendum is the governing law in Clause 9 and Clauses 11.3 of the Standard Contractual Clauses, and (d) Annex 1 to this Addendum are Annex 1 to the Standard Contractual Clauses, respectively. For the avoidance of doubt, the Standard Contractual Clauses will apply to Personal Data Processed by Crowdfire in the context of providing the Services to Customer that are transferred to (i) the United States when the transfer is not covered by a valid Privacy Shield certification, or (ii) any other country that does not provide an adequate level of protection under EU Data Protection Law.

7. **Sub-Processing.**

1.1. Customer acknowledges and agrees that Crowdfire may engage third-party Sub-Processors in connection with the performance of the Services.

1.2. Customer may only authorize a Sub-Processor to process the Personal Data:

1.2.1. subject to Customer's prior written consent where Crossfire has supplied Customer with full details of such Sub-Processor (and all other information requested by Customer);

1.2.2. provided that Customer has reviewed and consented to the Sub-Processor's contract (such contract to include terms which are not less protective as those set out in this DPA and any Instruction(s) received by Crowdfire); and

1.2.3. provided that the Sub-Processor's contract terminates automatically on termination of the Agreement for any reason.

7. **Security of the Processing; Confidentiality.**

7.1. Crowdfire must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. In assessing the appropriate level of security, Crowdfire must take 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 Data Subjects and the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed. In particular, Crowdfire will implement the security measures listed in Annex 1. Crowdfire must take steps to ensure that any person acting under its authority who has access to Personal Data is bound by enforceable contractual or statutory confidentiality obligation.

8. **Liability Towards Data Subjects.** Each Party agrees that it will be liable to Data Subjects for the entire damage resulting from a violation of EU Data Protection Law. If one Party paid full compensation for the damage suffered, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's part of responsibility for the damage. For that purpose, both Parties agree that Customer will be liable to Data Subjects for the entire damage resulting from a violation of EU Data Protection Law with regard to Processing of Personal Data for which it is a Controller, and that Crowdfire will only be liable to Data Subjects for the entire damage resulting from a violation of the obligations of EU Data Protection Law directed to Processor or where it has acted outside of or contrary to Customer's lawful instructions. Crowdfire will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

9. **Applicable Law**. The Processing of Personal Data under this Addendum is governed by the law of the jurisdiction in which Customer is established.

10. **Modification of this Addendum**. This Addendum may only be modified by a written amendment signed by each of the Parties.

11. **Termination.** The Parties agree that this Addendum is terminated upon the termination of the Service.

12. **Invalidity and Severability.** If any provision of this Addendum is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect any other provision of this Addendum and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

Crowdfire Inc.	**[Customer]**
Signature:	
Name: Moujhuri Guha	Name:
Title: HR	Title:
Date: 19th Aug 2020	Date:

ANNEX 1 – Data Security Measures

Customer will, as a minimum, implement the following types of security measures:

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, include:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of **one** master record per user, user master data procedures, per data processing environment;
- Encryption of archived data media.

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access personal data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure;
- Encryption.

4. Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Encryption/tunnelling;
- Logging;
- Transport security.

5. Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems;
- Audit trails and documentation.

6. Control of instructions

Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the instructions of Crowdfire include:

- Unambiguous wording of the contract;
- Formal commissioning (request form);
- Criteria for selecting the Processor.

7. Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan.

8. Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately include:

- Separation of databases;
- "Internal client" concept / limitation of use;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes.