# Data Processing Addendum

This Data Processing Addendum including its exhibits and appendices **("DPA")**, forms part of, is incorporated into, and made subject to the Community Brands Order Form, Community Brands Terms and Conditions, or similar agreement or other written or electronic agreement pursuant to which Community Brands HoldCo, LLC or one of its subsidiaries ("**Company**") sells software products to the undersigned customer of Company ("**Customer**") for certain services (collectively, the "**Service**") provided by Company (**"Agreements**"). Each of Customer and Company may be referred to herein as a "**party**" and together as the "**parties**."

By executing a Community Brands Agreement, Customer agrees to be bound by this DPA. The parties have agreed to enter into this DPA in order to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data as required by Global Data Protection Laws and governs the parties' processing of Personal Data for their business relationship from the date the last of the parties sign the Agreement until terminated as provided in this DPA. Customer entity entering into this DPA must be the same as the Customer entity party to the Agreements.

This Addendum applies where and only to the extent that Community Brands processes Personal Data on behalf of Customer.

## 1. Definitions

a. The following definitions are used in this DPA:

i. "**Affiliate**" means an entity that directly or indirectly controls, is controlled by or is under common control with an entity. "Control", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

ii. "**Global Data Protection Laws**" means all current laws and regulations applicable to the processing of Personal Data under the Agreements, including, but not limited to, laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland, the United Kingdom, Canada, Australia, and the United States of America, as applicable to the processing of Personal Data under the Agreement including (without limitation) the GDPR, the UK GDPR, the CCPA, the PIPEDA, and the Privacy Act 1988 and other relevant privacy laws and regulations in Australia, as applicable to the processing of Personal Data hereunder and in effect at the time of processor's performance hereunder.

iii. "**GDPR**" means the General Data Protection Regulation (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).

iv. "**UK GDPR**" means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

v. "**Personal Data**" means all data which is defined as "personal data," "personal information," or similar terms under Global Data Protection Laws and which is provided by Customer to Company to process on behalf of Customer.

vi. The terms "**process**," "**processing**," "**data subject**," "**sub-processor**," "**data protection impact assessment**," etc., shall have the meaning ascribed to them under applicable Global Data Protection Laws.

vii. "Restricted Transfer" means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data from Switzerland to any other country that has not been determined to provide adequate data protection by the Federal Data Protection and Information Commissioner or other competent Swiss authority.

viii. "Standard Contractual Clauses" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs") in the form set out in Exhibit 2 to this Addendum; and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("UK SCCs").

ix. “Sub-processor” means any Data Processor engaged by Community Brands to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement. Sub- processors may include third parties or Community Brands’ Affiliates.

**2. Status of the Parties**

a. The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature, and purpose of the processing, and the categories of data subjects, are as described in the Agreement.
b. Each party warrants in relation to Personal Data that it will comply (and will warrant that any of its personnel comply and use commercially reasonable efforts to warrant that its sub-processors comply), with Global Data Protection Laws. As between the parties, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Specifically, Customer shall have sole responsibility for complying with any applicable requirements under Global Data Protection Laws to determine the lawful basis for processing, provide data subjects with notice, obtain data subject consent, and respond to data subject requests.
c. In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby acknowledge and agree that Customer is the data controller and Company is the data processor.
d. Company is a “service provider” (as defined in CCPA §1798.140(v)) to Customer under the CCPA. For the purpose of clarity, within this DPA “controller” shall also mean “business”, and “processor” shall also mean “service provider”, to the extent that the CCPA applies. In the same manner, processor’s Sub-processor shall also refer to the concept of service provider.
e. Where appliable, in certain scenarios, the parties anticipate that Personal Data about a data subject under the age of 13 may be collected. The Children’s Online Privacy Protection Act (COPPA) governs this collection. Because Company provides certain services that are “solely for the benefit of students and the school system” and are specific to “the educational context,” the parties agree that Customer is responsible for obtaining appropriate parental consent for Company’s collection of such Personal Data.

**3. Company Obligations**

a. With respect to all Personal Data, Company:

i. will only process Personal Data in order to provide services under the Agreements, and only in accordance with: (i) this DPA, (ii) the Customer's written instructions as represented by the Agreements and this DPA, and (iii) as required by applicable laws;

ii. will not retain, use or disclose the Personal Data: (i) for any purpose other than providing services under the Agreements, including any “commercial purpose” (as defined in CCPA §1798.140(f); or (ii) outside of the direct business relationship between Company and Customer;

iii. will not “sell” (as defined in CCPA §1798.140(t)) the Personal Data;

iv. certifies that it understands and is willing to abide by the restrictions in California Civil Code Section 1798.140(w)(2)(A), as applicable;

v. will implement appropriate technical and organizational measures designed to provide a level of security appropriate to the risks that are presented by the processing of Personal Data, and in particular, the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such measures are set out in Annex II, which Customer has determined are appropriate;

vi. will take reasonable steps to ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under obligations of confidentiality;

vii. will, without undue delay after becoming aware of a confirmed breach involving Personal Data, notify Customer of any 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 by Company (a "**Security Breach**");

viii. will, upon Customer's reasonable request, promptly provide Customer with reasonable cooperation and assistance in respect of a Security Breach and reasonable information in Company's possession concerning such Security Breach insofar as it affects Customer;

ix. will, upon receiving any complaint, notice, or communication from any governmental entity (including government access requests or other disclosure orders where permitted by law), relating directly or indirectly to Company's processing of Personal Data or potential failure to comply with Global Data Protection Laws, to the extent permitted by law, promptly forward the complaint, notice, or communication to Customer and provide reasonable cooperation and assistance in relation to the same;

x. will promptly notify Customer if it receives a request from a data subject to access, rectify or erase that individual's Personal Data, or if a data subject objects to the processing of, or makes a data portability request in respect of, such Personal Data (each a "**Data Subject Request**"). Company shall not respond to a Data Subject Request without Customer's prior written consent except to confirm that such request relates to Customer, to which Customer hereby agrees. To the extent that Customer does not have the ability to address a Data Subject Request, then upon Customer's request Company shall provide reasonable assistance to Customer to facilitate such Data Subject Request to the extent able and in line with applicable law. Customer shall cover all costs incurred by Company in connection with its provision of such assistance;

xi. will, other than to the extent required to comply with applicable law, as soon as reasonably practicable following termination or expiry of the Agreements or completion of the Service, delete or return all Personal Data (including copies thereof) processed pursuant to this DPA.

**4. Sub-processing**

a. Customer grants a general authorization: (a) to Company to appoint other affiliates as sub-processors, and (b) to Company and its affiliates to engage third-party sub-processors for performance of the Service.

**5. Audit and Records**

a. Where applicable, Company will make available to Customer such information in Company's possession or control as Customer may reasonably request with a view to demonstrating Company's compliance with Global Data Protection Laws in relation to its processing of Personal Data.

**6. Data Transfers**

a. Company is headquartered in the United States and only processes data in the United States. As such, Company may transfer and process Customer Personal Data to countries where Company, its Affiliates or its Sub-processors maintain data Processing operations.

To the extent that Personal Data is transferred out of Canada or Australia, Company shall offer a "comparable level of protection," meaning protection that can be compared to the level of protection the personal information would receive if it had not been transferred.

b. European Data Transfers:

To the extent that the transfer of Customer Personal Data to Company is a Restricted Transfer of Personal Data, then:

i. In relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply in the form set out in the Appendix to this Addendum.
ii. In relation to Personal Data that is protected by the UK GDPR or the Swiss DPA, the EU SCCs will apply in the form set out in Section 2 of the Appendix to this Addendum.
iii. Before commencing a Restricted Transfer to a Sub-processor, Company shall enter into an agreement with a Sub-processor containing Standard Contractual Clauses in a form appropriate for processor-to-processor transfer, or alternatively, Company shall determine that the Sub-processor will have appropriate safeguards pursuant to Articles 46 or 47 of the EU GDPR and/or UK GDPR (as applicable) with respect to the Sub- processor's processing.

c. Where the Standard Contractual Clauses apply:

i. As between the parties, any claims brought under the Standard Contractual Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject or data protection authority under the Standard Contractual Clauses. Company will comply with the obligations of the 'data importer' in the Standard Contractual Clauses and Customer will comply with the obligations of the 'data exporter'.
ii. In the event of any conflict between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

**7. General**

a. This DPA is without prejudice to the rights and obligations of the parties under the Agreements which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Agreements, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

b. Company's liability under or in connection with this DPA (including under the Standard Contractual Clauses set out in the Appendix) is subject to the limitations on liability contained in the Agreements.

c. Except for the Standard Contractual Clauses, this DPA does not confer any third-party beneficiary rights, it is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

d. The choice of law and jurisdiction concerning this DPA and any action related thereto shall be consistent with and pursuant to the Agreements. In the absence of choice of law and jurisdiction selection, the parties shall mutually agree upon choice of law and jurisdiction.

e. This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. No modification of, amendment to, or waiver of any rights under the DPA will be effective unless in writing and signed by an authorized signatory of each party. This DPA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. Each person signing below represents and warrants that he or she is duly authorized and has legal capacity to execute and deliver this DPA. Each party represents and warrants to the other that the execution and delivery of this DPA, and the performance of such party's obligations hereunder, have been duly authorized and that this DPA is a valid and legally binding agreement on each such party, enforceable in accordance with its terms.

# APPENDIX

This Appendix applies to only to the personal data of data subjects governed by the EU and UK GDPR.

## STANDARD CONTRACTUAL CLAUSES

**Introduction**

Both parties have agreed on the following Contractual Clauses (the "**Clauses**") in order to adduce adequate safeguards with respect to protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex 1.

**Agreed Terms**

**1.** EU Standard Contractual Clauses Controller to Processor found here:https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en

**In response to Clause 9**

Use of sub-processors

(a) OPTION 2: The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in

advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s).

**In response to Clause 17**

Governing Law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the EU Member State where data exporter maintains its main place of business in the EU.

**In response to Clause 18**

Choice of forum and jurisdiction

(b) The Parties agree that those shall be the courts of the EU Member State where data exporter maintains its main place of business in the EU.

2. International Data Transfer Addendum to the European Commission's Standard Contractual Clauses found here:https://ico.org.uk/media/for-organisations/documents/4019535/addendum-international-data-transfer.docx

2.a. The amendments required by Section 2 above, include (without limitation):

i. References to the "Clauses" means this Appendix as it incorporates the Standard Contractual Clauses.
ii. Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer."

iii. References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.
iv. References to Regulation (EU) 2018/1725 are removed.
v. References to the "EEA", "Union", "EU" and "EU Member State" are all replaced with the "UK".
vi. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;
vii. Clause 17 is replaced to state "These Clauses are governed by the laws of the UK where the data exporter maintains its main place of business in the UK.
viii. Clause 18 is replaced to state:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."

IX. The footnotes to the Clauses do not form part of this Appendix.

2.b. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of the data exporter.

2.c. The Parties may amend this Appendix provided it maintains the appropriate safeguards required by Art 46 UK GDPR for the relevant transfer by incorporating the Standard Contractual Clauses and making changes to them in accordance with Section 2 above.

2.d. The Parties may give force to this Appendix (incorporating the Standard Contractual Clauses) in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the Contractual Clauses. If the Standard Contractual Clauses are not deemed as an appropriate lawful mechanism for UK Transfers, such UK Transfers may instead be governed by the standard contractual clauses for the transfer of personal data to processors or sub-processors established in third countries, as adopted by the European Commission under Directive 95/46/EC.

# ANNEX I

## A. LIST OF PARTIES

**Data exporter(s):**

Name: Customer (as identified in the Agreement).

Address: As identified in the Agreement.

Contact person's name, position and contact details: As identified in the Agreement.

Activities relevant to the data transferred under these Clauses:

Engagement of data importer to assist with services set forth in the Agreements.

Signature and date: These Standard Contractual Clauses shall be deemed executed by the Customer upon execution or acceptance of the Agreement.

Role (controller)

2. …

**Data importer(s):**

Name: Community Brands HoldCo, LLC (or a subsidiary of it)

Address: 9620 Executive Center Dr N #200, St. Petersburg, FL 33702

Contact person's name, position, and contact details: Attn: Legal Department – privacy@communitybrands.com

Activities relevant to the data transferred under these Clauses:

Processing data exporter's data for purposes set forth in the Agreements.

Signature and date: These Standard Contractual Clauses shall be deemed executed by Company upon execution or acceptance of the Agreement.

Role (processor)

2. …

## B. DESCRIPTION OF TRANSFER

**Data Exporter:**

The data exporter is (i) the legal entity that has entered into a contract with Company for provision of Services and executed the Clauses as a data exporter and (ii) all affiliates of such entity established within the EEA, which have purchased services from Company.

**Data importer:**

The data importer is Company, which processes Personal Data upon the instruction of the data exporter in accordance with the terms of the agreement between the data exporter and Company.

**Data Subjects:**

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

The data exporter may submit Personal Data to Company, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

1. Prospective customers, customers, suppliers, authorized agents, minors, subscribers, and vendors of the data exporter (who are natural persons);
2. Employees or contact persons of the data exporter's prospective customers, customers, subcontractors, business partners, and vendors (who are natural persons);
3. Natural persons authorized by the data exporter to use the services provided by Company to the data exporter.

**Categories of data:**

The personal data transferred concern the following categories of data:

The data exporter may submit Personal Data to Company, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:

1. Names, titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, professional life data, personal life data, connection data, or localization data (including IP addresses).

**Special categories of data (if appropriate):**

The parties do not anticipate the transfer of special categories of data.

**Processing operations**

The objective of the processing of Personal Data by Company is to provide the Service, pursuant to the Agreements. The personal data transferred will be subject to the following basic processing activities:

1. The duration of the processing will be: until the earliest of (i) expiry/termination of the Agreements, or (ii) the date upon which processing is no longer necessary for the purpose of eitherparty performing its obligations under the Agreements (to the extent possible).
2. The purpose(s) of the processing is/are: as necessary for the provision of the Service pursuant to the Agreements.
3. The types of Personal Data may include: names, titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, professional life data, personal life data, connection data, or localization data (including IP addresses).
4. Personal Data may concern the following data subjects:

    - Prospective customer, customers, vendors of Customer (who are natural persons), suppliers, authorized agents, and subscribers;
    - Employees or contact persons of Customer's prospective customers and Customer's current customers, subcontractors, business partners, and vendors (who are naturalpersons); and/or

- Natural persons authorized by Customer to operate on their behalf.

**C. COMPETENT SUPERVISORY AUTHORITY**

The EU Member State where data exporter maintains its main place of business in the EU.

# ANNEX II

## TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Data importer/sub-processor has implemented and shall maintain a security program in accordance with industry standards and Global Data Protection Laws including, but not limited to, laws and regulations of GDPR, the UK GDPR, the CCPA, the PIPEDA, and the Privacy Act 1988 and other relevant privacy laws and regulations in Australia. More specifically, data importer/sub-processor's security program shall include:

**Access Control of Processing Areas**

Data importer/sub-processor implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related (hardware) where the personal data are processed or used, including:

- Establishing security areas;
- Protection and restriction of access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- all access to the data center and/or operation center where personal data are hosted is logged, monitored, and tracked; and
- the data center and/or operation center where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

**Access Control to Data Processing Systems**

Data importer/sub-processor implements suitable measures to prevent their data processing systems from being used by unauthorized persons, including:

- use of adequate encryption technologies;
- identification of the terminal and/or the terminal user to the data importer/sub-processor and processing systems;
- automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events,
- monitoring of break-in-attempts (alerts); and
- all access to data content is logged, monitored, and tracked.

**Access Control to Use Specific Areas of Data Processing Systems**

Data importer/sub-processor commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the personal data;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;

- monitoring capability in respect of individuals who delete, add or modify the personal data;
- release of data only to authorized persons, including allocation of differentiated access rights and roles;
- use of adequate encryption technologies; and
- control of files, controlled and documented destruction of data.

**Availability Control**

Data importer/sub-processor implements suitable measures to ensure that personal data are protected from accidental destruction or loss, including:

- infrastructure redundancy; and
- backup is stored at an alternative site and available for restore in case of failure of the primary system.

**Transmission Control**

Data importer/sub-processor implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- certain highly confidential Personal data (e.g., personally identifiable information such as National ID numbers, credit or debit card numbers) is also encrypted within the system; and
- providing user alert upon incomplete transfer of data (end to end check); and
- as far as possible, all data transmissions are logged, monitored and tracked.

**Input Control**

Data importer/sub-processor implements suitable input control measures, including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of unique authentication credentials or codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- automatic log-off of user ID's that have not been used for a substantial period of time;
- proof established within data importer/sub-processor’s organization of the input authorization; and
- electronic recording of entries.

**Separation of Processing for Different Purposes**

Data importer/sub-processor implements suitable measures to ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users;

- modules within the data importer/sub-processor's data base separate which data is used for which purpose, i.e. by functionality and function;
- at the database level, data is stored in different normalized tables, separated per module, per Controller Customer or function they support; and
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data
- collected for specific purposes is processed separately.

**Documentation**

Data importer/sub-processor will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data importer/sub-processor shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Appendix Annex II.

**Monitoring**

Data importer/sub-processor shall implement suitable measures to monitor access restrictions to data importer/sub-processor's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- individual appointment of system administrators;
- adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the data importer/sub-processor and applicable laws;
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to data exporter upon request.

## ANNEX III

## LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

https://www.communitybrands.com/wp-content/uploads/2021/04/Sub-Processors_Community-Brands.pdf