DATA PROTECTION AGREEMENT

This DATA PROTECTION AGREEMENT (this "DPA"), dated effective _____, 2020, is entered into between _____ ("Client") and Brandlive, Inc. DBA Allhands ("Allhands"). Client and Allhands shall individually be referred to herein as a "party" and collectively as the "parties."

RECITALS

A. WHEREAS, this DPA establishes Brandlive's minimum data protection standards in connection with its' performance of services for Client, and is provided to Client for its' review, acknowledgment and acceptance;

B. WHEREAS, Client agrees that for Allhands to perform its' purposes and obligations under the applicable agreement(s), namely to provide Client's designated individuals, which may include Client's employees, prospective employees, suppliers, distributors, customers, members of its' board of directors and its' business partners, online marketing services, including but not limited to interactive video communications, audience chat, product merchandising, email notifications, productions, and mobile applications services (the "**Permitted Purpose**"), may collect, process, use, and/or transfer Personal Data (defined below) collected, obtained or received from Client to third parties for the Permitted Purpose;

C. WHEREAS, in order to comply with applicable Data Protection Laws (defined below), the parties wish to be bound by the terms of this DPA and to incorporate these terms and safeguards by reference into the agreement(s) governing the relationship between the parties; and

D. WHEREAS, Client hereby approves, accepts and agrees to Allhands' data privacy and protection practices as outlined herein.

NOW, THEREFORE, in consideration of mutual covenants contained herein, and in consideration of other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. **<u>Definitions</u>**. In addition to those definitions set forth elsewhere in this DPA, the following capitalized terms shall have the meanings set forth below. Capitalized terms not otherwise defined in this DPA shall have the meaning given to them in the Agreement.

1.1 "**Data Exporter"** means the controller who transfers the Personal Data, and under this DPA shall be Client.

1.2 "**Data Importer"** means the processor who agrees to receive from the Data Exporter, Personal Data intended for processing on its' behalf, and under this DPA shall be Allhands.

1.3 **"Data Protection Laws"** means all legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller, and all data protection and privacy laws in any jurisdiction, as applicable, including any amending or replacement legislation, and including (without limitation): (i) the California Consumer Privacy Act of 2018 (CCPA); (ii) the EU General Data Protection Regulation (2016/679) (GDPR); and (iii) the EU Privacy and Electronic Communications Directive 2002/58/EC as implemented in each jurisdiction.

1.4 "**Data Subjects**" means the Personal Data transferred that may concern employees, vendors, members, and/or customers of Client.

1.5 "**Personal Data**" means information associated with or relating to Client's customers, potential customers, suppliers, business contacts, employees and any other individual, collected, accessed, or

obtained by, or provided to Allhands in connection with Services provided under the an applicable service agreement(s), including for example any information relating to an identified or identifiable natural person or household ('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. An outline of Personal Data is attached hereto as **Schedule A**.

1.6 "**Processing**" 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, transfer, or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.7 **"Processing operations**" the Personal Data transferred will be subject to the processing activities identified in the applicable service agreement between the parties or as otherwise agreed by the parties in writing.

1.8 "**Security Breach**" means any act or omission that compromises either the security, confidentiality, or integrity of Personal Data, or the physical, technical, administrative, or organizational safeguards put in place by Allhands that relate to the protection of the security, confidentiality, or integrity of Personal Data, including without limitation any actual or potential unauthorized access, acquisition, collection, use, loss, destruction, compromise, disclosure, dissemination, ransom, damage, or alteration of any Personal Data and of any actual or potential security vulnerabilities potentially affecting the security of Client systems, the Services, or the privacy or security of individuals and, for the avoidance of doubt, includes a 'personal data breach' as defined in the GDPR.

1.9 "**Standard Contractual Clauses**" means the standard contractual clauses (controllers) for the purposes of compliance with Article 46 of the GDPR related to the transfer of Personal Data to controllers, processors or sub-processors established in third countries, which do not ensure an adequate level of data protection.

1.10 **"Subprocessor"** means any processor engaged by the Data Importer or by any other subprocessor of the Data Imorter who agrees to receive from the Data Importer or from any other subprocessor of the Data Importer Personal Data exclusively intended for processing activities to be carried out on behalf of the Data Exporter.

1.11 "**Technical and Organisational Security Measures**" means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. **Data Protection**. The parties agree to comply with the following data protection provisions with respect to the Services and Personal Data transferred between one another:

2.1 The parties acknowledge that in order to perform the Permitted Purpose, they must transfer Personal Data between one another. The parties acknowledge and agree that in performing their obligations set out therein they are each acting as an independent data controller strictly for the Permitted Purpose. In no event will the parties process the Personal Data as joint controllers.

2.2 Each party shall be individually and separately responsible for complying with their respective obligations under applicable Data Protection Laws as they apply to the performance of such party's obligations under the applicable agreement(s), and shall not, as far as is reasonable, do anything or

permit anything to be done which has the effect of placing the other party in breach of applicable Data Protection Laws. Without limiting the generality of the foregoing:

2.2.1. Allhands shall Process the Personal Data only as is necessary to fulfill the Permitted Purpose and perform its' obligations under the applicable agreement(s) entered into by the parties, unless Processing would otherwise be permitted by applicable Data Protection Laws, or unless required to do so by law to which the Allhands is subject, in which case Allhands shall inform Client in writing of that legal requirement before commencing Processing unless that law prohibits such information on important grounds of public interest.

2.2.2. Allhands shall inform Client if Allhands is of the opinion that an instruction of Client regarding Processing Personal Data infringes Data Protection Law.

2.2.3. Allhands shall implement and maintain appropriate Technical and Organizational Security Measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, or dissemination and which provide a level of security appropriate to the risk represented by its' Processing of Personal Data and the nature of the data to be protected, as may be more specifically set forth in the applicable service agreement(s) between the parties. Additionally, Allhands will have in place procedures so that any third party it authorizes to have access to the Personal Data, including processors and Subprocessors, will respect and maintain the confidentiality and security of the Personal Data.

2.2.4. Each party shall maintain adequate records of its' Processing activities, related to the Personal Data, and make available upon written request such records to the other party to the extent necessary for compliance or regulatory purposes.

2.2.5. Allhands shall obtain all necessary permissions from each Data Subject as required by applicable Data Protection Laws to allow it to Process the Personal Data: (i) to the extent permitted under applicable Data Protection Laws; (ii) as set out in its' privacy policies; and (iii) to the extent necessary to fulfill the obligations set out in the applicable service agreement(s). Client shall not transfer or share to Allhands any Personal Data from Data Subjects who have previously withdrawn their Processing consent with Client. Client shall immediately notify Allhands of any Data Subject's withdrawal of Processing consent. A breach of this Section shall be considered a material breach and grounds for termination.

2.2.6. Allhands may, at its election, appoint third party and Sub-processors to process Personal Data for the Permitted Purpose, provided that such processors: (a) agree in writing to process Personal Data in accordance with Allhands' documented instructions which are consistent with this DPA and the applicable service agreement; (b) implement appropriate Technical and Organizational Security Measures to protect the Personal Data against a Security Breach; and (c) otherwise provide sufficient guarantees that they will process the Personal Data in a manner that will meet the requirements of applicable Data Protection Laws. Allhands acknowledges and agrees that it shall remain liable to Client for a material breach of the terms of this DPA by a Subprocessors and other subsequent third party appointed by any Subprocessor that causes Client direct damage or harm. Allhands shall not be liable for a Subprocessors Security Breach that was not directly caused by Allhands.

2.2.7. Allhands shall provide notification to each Data Subject, as required and in accordance with applicable Data Protection Laws, that it is a Data Controller and of the data processing activities conducted pursuant to the applicable service agreement(s).

2.2.8. Allhands shall act as the primary point of contact for any requests from a Data Subject to exercise rights granted to such Data Subject under applicable Data Protection Laws with

respect to any Personal Data that Allhands collects and processes in its capacity as a Data Controller. Each party shall reasonably assist the other in handling and responding to any such request. Specifically, where a Data Subject has requested for their data to be ported, Client shall take steps necessary to verify the legitimacy of the request, identify and advise Allhands of the applicable record to be ported, and coordinate the transfer with the receiving parties.

2.3 Allhands processes all data through its' North America data centers. Allhands may offer features in its software sp Client can configure the Allhands product to restrict Personal Data collection originating from the European Union, Switzerland or the United Kingdom, so that data is not processed outside either the European Economic Area (EEA) or the United Kingdom, or any other territory in which restrictions are imposed on the transfer of Personal Data across borders under applicable Data Protection Laws, without the express prior written consent of Client. Where Allhands will process Personal Data originating in the EEA or the United Kingdom, Allhands has or will execute Standard Contractual Clauses approved by the European Commission.

3. <u>Technical Security Safeguards.</u>

3.1 Allhands will implement and maintain appropriate safeguards designed to (a) ensure the security, confidentiality and integrity of Personal Data and (b) protect against anticipated threats or hazards to, or unauthorized access to or use or disclosure of such Personal Data. Such safeguards (including those relating to how the Personal Data is collected, accessed, used, stored, disposed of, and disclosed) shall include an information security program that meets the requirements of applicable law regulations and government-issued business guidance (such as ISO 27002, ITIL or COBIT and the guidance issued by the Federal Trade Commission), including administrative, physical, and technical safeguards required thereunder, and that is no less rigorous than accepted industry standards and practices. The information security program shall include, without limitation, regular backups of Personal Data for storage off-site, and encryption of all Personal Data while "at rest" and in transit across public networks or wirelessly. Allhands will ensure the appropriate safeguards required above are also utilized by any Subprocessors engaged by Allhands in the delivery of the Services and use for the Permitted Purposes.

3.2 Allhands shall take reasonable steps to ensure that it does not send, distribute or store material containing software viruses, worms, Trojan horses or other harmful code, files, scripts, agents or programs in connection with the Services or any licensed software.

3.3 Allhands shall take reasonable steps to ensure that Personal Data is pseudonymized and encrypted.

3.4 Allhands shall take reasonable steps to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services.

3.5 Allhands shall take reasonable steps to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident or Security Breach.

3.6 Allhands shall incorporate a process for regularly testing, assessing and evaluating the effectiveness of Technical and Organizational Security Measures for ensuring the security of the Processing and storing of Personal Data.

3.7 Allhands shall employ appropriate encryption when transmitting Personal Data on public or wireless networks. Allhands shall encrypt during storage any and all Personal Data and other data deemed highly sensitive by Client, such as authentication credentials and cryptographic keys.

3.8 Allhands shall limit access to Client's networks, information systems owned or operated by or on behalf of Client, and Client Personal Data to employees and contractors that require access to perform Allhands' obligations under this DPA and any service agreement(s) between the parties consistent with the concept of least privilege. Allhands shall implement and maintain a formal and documented process for granting, periodically reviewing, and revoking access to all systems that process or store Client's Personal Data.

3.9 Allhands shall maintain appropriate network security measures, including but not limited to firewalls to segregate Allhands' internal networks from the internet, risk-based network segmentation, and intrusion prevention or detection systems to alert Allhands to suspicious network activity.

3.10 Allhands shall securely operate IT infrastructure and applications that process, store, or transmit Personal Data by deploying key operational management controls, including, without limitation, the maintenance of system and network documentation, employment of a secure change management process, the implementation of an incident management process, and ensuring that local logging has been enabled on all systems and networking devices to capture detailed information such as event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

3.11 Where technically feasible, Allhands shall deploy anti-malware software on all IT systems that access, store, or process Personal Data, Client's networks, or information systems owned or operated by or on behalf of Client. Allhands shall ensure that all such anti-malware software has the latest signatures and definition files. Allhands shall also deploy adequate mechanisms to detect and issue alerts about potential unauthorized activity and respond appropriately to protect all systems that process, store, or transmit Client's Personal Data.

3.12 Allhands shall implement appropriate safeguards and controls that restrict unauthorized physical access to facilities containing information systems, devices, and other equipment used to access or otherwise process Client's Personal Data, Client's networks, or information systems owned or operated by or on behalf of Client.

3.13 Allhands shall take reasonable steps to ensure that systems which process Client's Personal Data or access Client's networks or information systems owned or operated by or on behalf of Client employ strong password complexity rules, and shall employ the following additional safeguards: Passwords shall be configured to expire every 90 days or less, systems shall lockout after three failed login attempts, and systems shall enable O/S screen saver locks after a period of 15 minutes of inactivity.

3.14 Allhands shall remove or disable non-essential functionality (i.e., hardening each system) such as scripts, drivers, features, subsystems, or file systems (e.g., unnecessary web servers, default, or sample files, etc.). Allhands shall ensure that all software used in its information systems and infrastructure maintains up-to-date security patches and upgrades.

3.15 Allhands shall adhere to industry accepted Software Development Lifecycle (SDLC) principles and secure coding practices with respect to the development and maintenance of application(s) used to store, process, or transmit Client's Personal Data

4. <u>Security Breach Notification and Cooperation.</u>

4.1 In the event that either party becomes aware of a Security Breach of its' systems relating to Personal Data, and where required under applicable Data Protection Laws, the affected party shall notify the appropriate supervisory authority(ies) and/or affected Data Subjects within the timelines set out under applicable Data Protection Laws. Both parties shall provide the other with all relevant information regarding the Security Breach or incident including (i) the nature of the incident and, where possible, the categories and approximate number of Data Subjects concerned and the

categories and approximate number of Personal Data records concerned, and explain the impact of such Personal Data Breach upon the other party and the Data Subjects whose Personal Data is affected by such Personal Data Breach; (ii) in no case delay notification because of insufficient information but instead provide and supplement notifications as information becomes available; and (iii) in cooperation with the other party, use its' best efforts to investigate such Personal Data Breach and take all necessary and appropriate corrective action to remedy such breach and prevent a recurrence of such breach.

4.2 Both parties agree to reimburse the other party for the reasonable expenses incurred in responding to and mitigating any damages caused by any Security Breach, including, but not limited to, (i) third party services to be provided to or on behalf of affected individuals or entities, (ii) providing a credit-monitoring service for affected individuals if deemed necessary in the affected party's sole discretion, (iii) providing notices to affected individuals, (iv) providing notices and information to appropriate law enforcement agencies and government regulatory authorities as reasonably necessary to comply with applicable laws and/or any requests from law enforcement or government agencies, (v) reasonable attorneys' fees and costs, and (vi) any other reasonable expenses incurred by the affected party to comply with applicable Data Protection Laws, laws and/or requests from law enforcement or government agencies.

4.3 Both parties agree to assist with and/or perform all remediation efforts that are required by applicable law or by any governmental authority in similar circumstances, regardless of whether applicable law explicitly imposes such remediation obligations on one part of the other or both. Such remediation efforts may include without limitation, investigation and resolution of the causes and impacts of the Personal Data Breach; development and delivery of notices approved by the other party to affected individuals; provision of free credit reports, credit monitoring and repair, and identity restoration products for affected individuals, and/or such other measures that the affected party determines are reasonable and commensurate with the nature and level of severity of the Personal Data Breach (collectively, "Remediation Measures").

5. **Limitation of Liability.** Each party shall be liable to the other party for damages it causes by any breach of these terms. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to Data Subjects for damages it causes by any breach of third-party rights under these terms. This does not affect the liability of the Data Exporter under its' Data Protection Law.

6. **Termination.** Either party may terminate this DPA upon 60 days written notice, or upon a material breach with failure to cure within 30 days of notice. This DPA shall automatically terminate upon the termination of an applicable service agreement(s) entered into between the parties. In the event of a discrepancy between the terms of this DPA and the applicable service agreement(s), the applicable service agreement(s) shall have precedence.

7. **General**.

7.1 **Choice of Law.** This DPA and all obligations arising out of or in connection with it shall be governed by the laws of the State of Oregon, without regard to its conflict or choice of law provisions. Any dispute with Allhands, or its' officers, directors, employees, agents or affiliates, arising under or in relation to these terms shall be resolved exclusively through the state and federal courts within the county of Multnomah in the State of Oregon.

7.2 **Injunctive Relief.** Each party acknowledges and agrees that the obligations and promises of each party under this DPA are of a unique intellectual character that gives them particular value. Each party further acknowledges and agrees that its' breach of any of the obligations and promises contained in this DPA may result in irreparable and continuing damage to the other party for which there is no adequate remedy at law and, in the event of such breach, such non breaching party will be entitled to seek injunctive relief and/or a decree for specific performance, without having to post a bond, and such other and further relief as may be proper (including monetary damages if appropriate).

7.3 **Entire Agreement.** This DPA, together with any applicable service agreement(s), constitute the complete and exclusive understanding and agreement between the parties regarding data protection and Processing and supersede all prior or contemporaneous agreements or understandings, written or oral, relating to their subject matter.

7.4 **Disclosure of DPA.** The parties acknowledge that either party may be required to produce this DPA to the relevant EU supervisory authority or its' works council and that production of this DPA, in such circumstance, shall not be deemed a violation of any confidentiality obligations set forth in this DPA or any applicable service agreement.

IN WITNESS WHEREOF, the parties have agree on these terms intended to outline adequate safeguards, practices, and responsibilites with respect to the protection of personal data, privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the Personal Data specified herein.

BRANDLIVE, INC. DBA ALLHANDS	CLIENT
By:	By:
Name: Sam Kolbert-Hyle	Name:
Title: CEO	Title:
Date:	Date: