Data Processing Addendum

Last updated: July 20, 2022

This Data Processing Addendum ("DPA") forms part of, and is incorporated into that certain STORE PLAN AGREEMENT, INSERTION ORDER AGREEMENT, or a certain other agreement, entered into by and between Brand and Leap (the "Main Agreement"), for the purchase of certain services from Leap (identified either as "Services" or otherwise in the Main Agreement, and hereinafter defined as "Services"). This DPA is applicable to the extent the Parties' Process Personal Data (as those terms are defined below), and effective on the date the Main Agreement is entered into (the "DPA Effective Date").

Any conflict shall be resolved by giving effect to such in the following order of precedence, unless otherwise expressly set forth in this DPA: (1) Data Protection Law; (2) this DPA; and (4) the Main Agreement.

1. **Definitions.** Capitalized terms used in this DPA that are not otherwise defined herein will have the same meaning ascribed to them as set forth in the Main Agreement or in Data Protection Laws.
   1.1. "California Consumer Privacy Act of 2018" or "CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations, and any amendments, modifications, or successors thereto.
   1.2. "Brand Data" means any electronic data that is provided to, collected by, stored, maintained, or Processed by, Leap in connection with the Services including, but not limited to: (i) Brand Confidential Information; and (ii) Personal Data.
   1.3. "Data Protection Law(s)" means any statute, law, rule, regulation, order by any governmental body, or industry standard, directly applicable to Brand, or Leap in its performance of the Services, such as, but not limited to: (i) the EU and UK Data Protection Laws; and (ii) the CCPA.
   1.4. "Data Subject" means: (i) an identified or identifiable natural person who is in the European Economic Area (EEA) or whose rights are protected by the GDPR; or (ii) a "Consumer" as the term is defined in the CCPA.
   1.5. "Enforcement Agency" means: (i) a Supervising Authority under the GDPR; (ii) the Attorney General of the State of California; or (iii) any government or any agency, bureau, commission, court, department, official, political subdivision, tribunal, board or other instrumentality of any administrative, judicial, legislative, executive, regulatory, police or taxing authority of any government, whether federal, state, regional, provincial, local, domestic or foreign, with jurisdiction over the enforcement of Data Protection Laws.
   1.6. "EU and UK Data Protection Laws" means (i) Regulation 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 ("General Data Protection Regulation" or "GDPR"), as transposed into domestic legislation of each Member State and the laws implementing the GDPR; and (ii) the GDPR as implemented or adopted under the laws of the United Kingdom.

1.7. "Personal Data" means a subset of the Brand Data that: (i) relates to an identified or identifiable individual, and includes, but is not limited to, addresses, phone numbers, passport numbers, driver's license numbers, user names, passwords, credit or debit card numbers, bank account numbers, other financial account numbers, personal identification numbers, dates of birth, Social Security Numbers, or other unique identification information; (ii) is considered GDPR Personal Data; or (iii) is considered CCPA Personal Information.

1.8. "Personnel" means any natural person acting under the authority of a Party.

1.9. "Security Breach" means in connection with the Services: (i) the loss, misuse, inadvertent, unauthorized, and/or unlawful disclosure, Processing, alteration, corruption, sale, rental, or destruction of Personal Data; (ii) Personal Data Breach as set forth under the GDPR; or (iii) an unauthorized access and exfiltration, theft, or disclosure of nonencrypted or nonredacted CCPA Personal Information.

2. Roles

2.1. Brand and Leap acknowledge and agree that in circumstances where Brand is providing Personal Data to Leap on its own behalf for Processing, Brand is a Controller, and appoints Leap as a Processor to Process such Personal Data.

2.2. In certain circumstances, Brand and Leap may jointly determine the purposes and means of Processing, in which case, the Parties shall be joint Controllers. The Parties agree to their respective Joint Controller obligations as set forth in Section 3.7 and further agree to determine their respective responsibilities for compliance with the obligations under the GDPR as set forth in Schedule 1.

2.3. The Parties acknowledge and agree that in other circumstances Brand may be a Processor, in which case Brand appoints Leap as another processor (or as a Subprocessor to Brand), which shall not change the obligations of either Brand or Leap under this DPA, as Leap will remain a Processor with respect to the Brand in such circumstances.

2.4. To the extent the Parties are subject to the CCPA, Leap is a CCPA Service Provider to Brand.

3. Processing of Personal Data

3.1. Where required under Data Protection Laws, the subject matter, nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects may be set out in Schedule 1, which is an integral part of this DPA.

3.2. If Leap is a Processor, Leap, at all times, shall Process Personal Data for the purposes set forth in this DPA and only in accordance with the lawful, documented instructions of Brand, and in the context of a Leap's ongoing business relationship with the Brand, except where otherwise required by applicable law. This DPA sets out Brand's complete instructions to Leap in relation to the Processing of Personal Data.

3.3. Brand:

a) Shall be solely responsible for, and represents and warrants that, any documented instructions it provides hereunder shall comply with Data Protection Laws, including;

b) Acknowledges and agrees that Brand (and not Leap) controls the nature and contents of Brand Data (including any Personal Data therein);

c) Represents and warrants that on the DPA Effective Date and during the term of this DPA: (i) Personal Data has been and will be collected and Processed by Brand in accordance with applicable Data Protection Laws; (ii) that it has the full authority

under Data Protection Law to provide such data to Leap for the Processing contemplated by this DPA, and the Processing of Personal Data in accordance with this DPA by Leap will not violate applicable Data Protection Laws; (iii) Brand will take all steps necessary to ensure it achieves the foregoing, including without limitation, by providing Data Subjects with appropriate privacy notices, obtaining any required consent, and ensuring that there is a lawful basis for Leap to Process Personal Data; and (iv) Brand shall provide Data Subjects with appropriate opt-outs where applicable under the Data Protection Laws, and shall inform Leap of any exercise of such rights by a Data Subject.

3.4. Any Processing required outside of the scope of the rights and obligations set forth under this DPA will require prior written agreement of the Parties, and Brand may issue additional instructions to Leap as it deems necessary to comply with Data Protection Law. Additional instructions must be set forth in a written instrument mutually agreed to by the Parties. Brand shall be responsible for any additional fees, or costs arising from any such additional instructions.

3.5. Leap, as a Processor or Service Provider, is prohibited from: (i) Selling Personal Data; (ii) Processing, retaining, using, or disclosing Personal Data for a commercial purpose other than providing the Services; and (iii) Processing, retaining, using, or disclosing the Personal Data outside of this DPA between Leap and Brand.

3.6. Leap understands the prohibitions outlined in Section 3.6, and certifies that it understands and shall comply with the same.

3.7. To the extent the Parties are Joint Controllers, the following applies:

a) Leap is solely responsible for the Processing of Operations Data (as defined in the Agreement) in the context of operating, maintaining and improving the Leap Services.

b) Leap shall ensure that such Operations Data is appropriately secure consistent with industry standards having regard to the state of the art and the costs of implementation.

c) Leap and Brand are jointly responsible for the Processing of Operations Data for the purpose of operating, improving, and maintain Store Locations, whereby the Parties agree that the responsibilities are divided between the Parties as follows:

3.7.c.1. Each Party is responsible for the security and data transfer obligations in respect of the Processing of the Operations Data, which include responsibility for: maintaining security for the Processing of Operations Data for the purpose of Store operations, consistent with industry standards having regard to the state of the art and the costs of implementation; and ensuring data transfer mechanisms are in place where Operations Data is transferred out of the EEA for the purpose of Store operations.

3.7.c.2. Brand is responsible for the material compliance of any onward transfer of information in Bran's possession or custody and in accordance with applicable Data Protection Law, which includes responsibility for: informing Individuals to whom the Operations Data relates and obtaining their consent, if applicable; obtaining any other required approvals from a regulatory or supervisory authority; responding to any access and correction requests of Individuals to whom the Operations Data relates; determining the scope of the data included

in the report; and any further Processing or onward transfer by Brand of the Operations Data made available to Brand in the Brand Service Report.

d) Brand shall ensure that the Operations Data is used only for the following purposes:

3.7.d.1. assisting in complying with legal duties and regulations which apply to the Brand;

3.7.d.2. performing a statutory role as a governmental organization;

3.7.d.3. performing law enforcement duties; or

3.7.d.4. if the Brand is processing special categories of data, including personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, the commission or alleged commission of any offence and the related disposition or sentence, and the processing of data concerning health or sex life ("Sensitive Data"), it shall only process it for the purpose of preventing fraud or a similar crime.

4. Subprocessing

4.1. Brand authorizes and instructs Leap to appoint Subprocessors (and permits each Subprocessor to appoint additional Subprocessors) in accordance with this Section 4.

4.2. As of the DPA Effective Date, Brand hereby authorizes and instructs Leap to engage those Subprocessors set out at https://www.leapinc.com/legal/data-processing-addendum-and-subprocessor-list (the "Subprocessor List"). The Subprocessor List may be updated from time to time. The Subprocessor List shall include the name and location of, and a brief description of the Processing undertaken by, each current Leap Subprocessor.

4.3. Brand acknowledges and agrees that Leap may engage additional Subprocessors. In accordance with the Data Protection Laws, Leap shall enter into a written contract or other legally binding agreement with such Subprocessors imposing the same obligations set forth in this DPA, upon such Subprocessors. At least ten (10) calendar days prior to Leap engaging any new Subprocessor(s), Leap shall provide notice to Brand of such change(s), and Brand shall have five (5) days from such notice to object to such change(s) by providing objective, justifiable grounds related to the ability of such Subprocessor(s) to adequately protect Personal Data in accordance with this DPA. Leap will have the right to cure the objection through any options in its sole discretion.

4.4. If any Subprocessor fails to fulfill its obligations under Data Protection Laws, or this DPA, Leap will be fully liable to Brand for the performance of such obligations.

5. International Data Transfers and SCCs

With regard to International Data Transfer that would be prohibited by EU and UK Data Protection Laws, the transfer mechanisms listed below shall apply to such transfers and can be directly enforced by the Parties to the extent such transfers are subject to Data Protection Laws.

5.1. The SCC Controller to Processors Transfer Clauses. Where Brand is a Controller and a data exporter of Personal Data and Leap is a Processor and data importer in respect of that Personal Data, then the Parties shall comply with the SCC Controller to Processors Transfer Clauses, subject to the additional terms set forth below.

5.2. The SCC Processor to Processor Transfer Clauses. Where Brand is a Processor acting on behalf of a Controller and a data exporter of Personal Data and Leap is a Processor and data importer in respect of that Personal Data, the Parties shall comply with the terms of

the SCC Processor to Processor Transfer Clauses, subject to the additional terms set forth below.

5.3. The SCC Controller to Controller Transfer Clauses. Where Brand and Processor jointly determine the purposes and means of processing Personal Data, then the Parties shall comply with the SCC Controller to Controller Transfer Clauses, subject to the additional terms set forth below.

5.4. Docking clause. The option under clause 7 of the SCCs shall not apply.

5.5. The Annexes of the SCCs shall be completed as follows:

a) The contents of Schedule 1 to this DPA shall form Annex I to the Standard Contractual Clauses

b) The contents of Section 6 to this DPA shall form Annex II to the Standard Contractual Clauses.

c) The contents of Schedule 2 to this DPA shall form Annex III to the Standard Contractual Clauses (which shall not be applicable to the Controller to Controller SCCs).

5.6. The Standard Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

6. Security

6.1. Taking 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 natural persons, Leap shall implement technical and organizational measures to ensure a level of security appropriate to the risks presented by the Processing (collectively, the "Technical and Organizational Security Measures"), including:

a) encryption and pseudonymization of Personal Data;

b) measures to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing;

c) measures to detect Security Breaches in a timely manner;

d) measures to restore the availability and access to Personal Data in a timely manner in the event of an incident; and,

e) processes for regularly testing, assessing and evaluating the effectiveness of the security measures.

7. Security Breach

7.1. Leap will notify Brand without undue delay, and in any case, within seventy-two (72) hours, upon Leap becoming aware of a Security Breach. Leap's notification of or response to a Security Breach under this Section 7 will not be construed as an acknowledgement by Leap of any fault or liability with respect to the Security Breach.

7.2. Any notification in accordance to Section 7.1, shall, to the extent known within the notification window: (i) describe the nature of the Security Breach, including, where possible, the categories and approximate number of affected data subjects, and the

categories and approximate number of personal data records concerned; (ii) the name and contact details of a contact person at Leap who can provide additional information; (iii) describe, to the extent known, the likely consequences of such Security Breach; and (iv) describe proposed mitigation efforts, as applicable.

7.3. Leap will make commercially reasonable efforts, in accordance with its security incident management policies and procedures, to identify the cause of such Security Breach, and provide Brand with sufficient information to allow Brand to meet its obligations under Data Protection Laws to report or inform Data Subjects of the Security Breach.

8. Assistance

8.1. Taking into account the nature of the Processing, Leap may reasonably assist Brand, by implementing appropriate technical and organizational measures, for fulfilment of Brand's own obligations under Data Protection Laws, including:

a) complying with Data Subjects' requests to exercise Data Subject Rights;

b) replying to inquiries or complaints from Data Subjects; and

c) replying to investigations and inquiries from Enforcement Agencies.

8.2. Unless prohibited by Data Protection Laws, Leap shall inform Brand without undue delay if Leap:

a) receives a request, complaint or other inquiry regarding the Processing of Personal Data from a Data Subject or Enforcement Agency;

b) receives a binding or non-binding request to disclose Personal Data from law enforcement, courts or any government body;

c) is subject to a legal obligation that requires Leap to Process Personal Data in contravention of Brand's instructions; or

d) is otherwise unable to comply with Data Protection Law or this DPA.

8.3. Unless prohibited by applicable law, Leap shall obtain Brand's written authorization before responding to, or complying with any requests, orders, or legal obligations referred to in Section 8.2.

9. Accountability

9.1. Leap shall maintain records of all Processing of Personal Data, including at a minimum the categories of information required under Data Protection Law, and must provide a copy of such records to an Enforcement Agency upon request and without undue delay.

9.2. Leap shall not be responsible for assessing any instruction or verifying the lawfulness of any instructions from Brand for the Processing of Personal Data. Leap may inform Brand if Leap believes that an instruction of Brand violates Data Protection Law. Leap may suspend Processing in its discretion, until Brand has modified or confirmed the lawfulness of the instructions in writing.

10. Data Protection Impact Assessment and Prior Consultation

At Brand's request, Leap shall provide reasonable assistance to Brand with any data protection impact assessments and prior consultations with Supervisory Authorities or other competent data privacy authorities, as required by applicable Data Protection Laws, and in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the Parties.

11. Audit

11.1. To the extent required under applicable Data Protection Laws, Leap will:

a) make available to Brand on request information that is reasonably necessary to demonstrate compliance with this DPA;

b) allow for and contribute to audits, including inspections, by an auditor mandated by Brand in relation to the Processing of the Personal Data by Leap.

11.2. Information and audit rights of Brand only arise under this Section 11 to the extent:

a) Leap Processes Personal Data; and

b) this DPA, and the Main Agreement do not otherwise give Brand information and audit rights meeting the relevant requirements of applicable Data Protection Laws (including, where applicable, Article 28(3)(h) of the GDPR).

11.3. Brand may only mandate an auditor for the purposes of this Section 11 if the auditor is approved by Leap in writing, such approval not to be unreasonably withheld.

11.4. Brand shall give Leap reasonable notice of any audit or inspection to be conducted under Section 11 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing any damage, injury, or disruption to Leap's premises, equipment, Personnel, and business while its Personnel are on those premises in the course of such an audit or inspection.

11.5. Any audits conducted in accordance with Section 11.1 – 11.4 shall be conducted during Leap's normal business hours, upon reasonable prior notice, and no more frequently than once per year during the term of the Main Agreement, unless in response to a Security Breach or as may be required by a Supervisory Authority.

12. Termination and Return of Personal Data

12.1. This DPA shall be in force from the DPA Effective Date, and shall remain in force until termination or expiration of this DPA or the Main Agreement, whichever is earlier (the "Termination Date").

12.2. Subject to Section 12.3, Leap shall without undue delay, and in any event no later than thirty (30) days of the Termination Date, render unrecoverable or return Personal Data in accordance with Leap's security practices.

12.3. After the Termination Date, Leap has no obligation to retain, and will render unrecoverable, such data in accordance with Leap's security practices.

12.4. Leap and each Subprocessor may retain Personal Data to the extent required by applicable laws and only to the extent and for such period as required by applicable laws.

12.5. At Brand's reasonable request, Leap shall provide written certification to Brand that it has fully complied with this Section 12.

13. General Terms

13.1. *Governing law and jurisdiction*

a) The Parties hereby submit to the choice of jurisdiction stipulated in the Main Agreement with respect to any disputes or claims arising under this DPA, including disputes regarding its existence, validity, or termination or the consequences of its nullity.

b) If the Main Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this DPA, the parties agree that the courts of either (i) Illinois; or (ii) where the Main Agreement designates the United Kingdom as having exclusive jurisdiction, the United Kingdom, shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

13.2. *Changes to Data Protection Laws; Severance*

a) If any variation is required to this DPA as a result of changes to Data Protection Laws, then either Party may provide written notice to the other Party of that change in law.

b) The Parties will discuss and negotiate in good faith any necessary variations to this DPA to address such changes.

c) If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

14. Indemnification; Liability

14.1. Each Party is fully liable to the other Party for any infringements of Data Protection Law or this DPA, including any acts or omissions by the respective Parties' Personnel.

14.2. A Party (the "Indemnifying Party") shall defend, indemnify, and hold harmless the other Party, its affiliates, and each of their partners, officers, directors, employees, customers, contractors, and agents from and against any and all third party claims, expenses, costs (including reasonable attorneys' fees), penalties, settlements, and damages arising out of or related to Indemnifying Party's breach of its obligations set forth in this DPA, or Indemnifying Party's violation of the Data Protection Laws.

14.3. For the avoidance of doubt, as between the Parties, each Party's liability and remedies under this DPA are subject to the aggregate liability limitations and damages exclusions set forth in the Main Agreement.

15. Modifications

15.1. This DPA may only be modified by a written amendment signed by both Brand and Leap.

Schedule 1

Parties and Details of the Personal Data and Processing

1. List or Parties
    a. Data Importer:
        i. Name: Leap Services, Inc.
        ii. Address: _____
        iii. Contact person's name, position and contact details: _____
        iv. _____
    b. Data Exporter: As set forth on the SIGNATURE PAGE.
        i. Activities relevant to the data transferred under these Clauses:

        _____

        _____

        Signature and date: _____
        ii. Role (controller/processor): CONTROLLER
2. Subject matter and duration of the Processing of Brand Personal Data:
3. Nature and purpose of the Processing of Brand Personal Data:
4. Categories of Brand Personal Data to be Processed:
5. Special Categories of Brand Personal Data to be Processed (if any):