# ***DATA PROCESSING ADDENDUM (U.S.)***

This Data Processing Addendum, including any Appendices (collectively, the "**Addendum**"), forms part of the Terms & Conditions of Use Agreement (the "**Service Agreement**"), or any other written or electronic agreement between Hertza L.L.C., a Nevada limited liability company, doing business as "ZeroBounce", and having its principal place of business at 10 E. Yanonali St., Santa Barbara, California 93101 (hereinafter to be referred to as: the "**Data Processor**" or "**ZeroBounce**") and the company whose information has been provided as part of the registration process (hereinafter to be referred to as: the "**Data Controller**" or "**Customer**"). Data Processor and Data Controller are collectively referred to herein as the "**Parties**".

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Service Agreement. Except as modified below, the terms of the Service Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Service Agreement. Except where the context requires otherwise, references in this Addendum to the Service Agreement are to the Service Agreement as amended by, and including, this Addendum.

1. **Subject matter of this Data Processing Addendum**
   - 1.1 This Data Processing Addendum applies exclusively to the processing of personal data in the United States in the scope of the Terms and Conditions of Use Agreement of even date hereof between the Parties for the provision of the ZeroBounce services ("Services") (hereinafter to be referred to as: the "**Service Agreement**").
2. **Definitions**
   - 2.1 The term "Applicable Law(s)" means all applicable United States federal or state privacy and data protection laws including, without limitation, the California Consumer Privacy Act of 2018 ("CCPA"), Cal. Civ. Code Section 1798.100, et seq., as may be amended from time to time (including but notlimited to those amendments enacted by the California Privacy Rights Act of 2020 ("CPRA")); Colorado Privacy Act; Connecticut Data Privacy Act; Delaware Personal Data Privacy Act; Florida Digital Bill of Rights; Indiana Consumer Data Protection Act; Iowa Act Relating to Consumer Data Protection; Maryland Online Data Privacy Act; Montana Consumer Data Privacy Act; Nebraska Data Privacy Act; New Hampshire Data Privacy Act; New Jersey Data Privacy Law; Oregon Consumer Privacy Act; Tennessee Information Protection Act; Texas Data Privacy and Security Act; Utah Consumer Privacy Act; Virginia Consumer Data Protection Act; and other analogous federal, state, or local privacy, data protection, information security, or related laws or regulations.
   - 2.2 Terms such as "Processing", "Personal Data", "Data Controller", and "Processor" shall have the meaning ascribed to them by Applicable Laws.
3. **Details of the Transfer**

3.1 Insofar as the Data Processor will be processing Personal Data subject to Applicable Laws on behalf of the Data Controller in the course of the performance of the Service Agreement with the Data Controller, the terms of this Addendum shall apply.

3.1.1 **Customer Validation Data:** To the extent that Data Controller requires that Customer Validation Data, be processed and stored in the European Union, Data Controller must utilize Data Processor's EU-only endpoint: api-eu.zerobounce.net (http://api-eu.zerobounce.net/). Any Personal Data submitted to Data Processor through other endpoints or means may be processed and stored in any country where Data Processor maintains its servers, namely, the United States and the European Union. The categories of Customer Validation Data to be processed are identifiers and may include the following: first name; last name; gender; city; state; country; Internet Protocol (IP) Address information and geolocation data; email addresses; and associated metadata related to email usage or validation results. The types of data subjects whose information will be processed are individuals, namely the Data Controller's customers, contacts, subscribers, end-users, or other individuals whose data is being processed based on contractual necessity, or who have consented to the processing of their personal data. The purposes for which the Customer Validation Data will be processed include: provision of the ZeroBounce Services, including but not limited to, validation of email lists for deliverability; removal of known email complainers, abusers and spam traps from email address lists; deliverability toolkit services; and to perform any additional services requested by Data Controller.

3.1.2 **Customer Registration Data:** The categories of Customer Registration Data to be processed are identifiers, protected classifications, and commercial information and may include the following: Customer's first name, last name, company name, gender, city, state, country, Internet Protocol (IP) address information, billing information, and the Customer's email address. The types of data subjects whose information will be processed are individuals, namely, the Data Controller, who consents to the processing of their Personal Data in accordance with the provision of the Services. The purposes for which the Customer Registration Data will be processed include: provision of the ZeroBounce Services and to support Customer's use of the Services; sharing with Processor's third party partners to market additional and/or integrating services that may be of interest to Customer; and to perform any additional services requested by Data Controller.

## 4. The Data Controller and the Data Processor

4.1 The Data Controller will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Data Processor. The Data Processor will process the Personal Data only as set forth in Data Controller's written instructions.

4.2 The Data Processor will only process the Personal Data on documented instructions of the Data Controller in such manner as – and to the extent that – this is appropriate for the provision of the Services, except as required to comply with a legal obligation required by Applicable Laws to which the Data Processor is subject. In such a case, the Data Processor shall inform the Data Controller of that legal obligation before processing, unless the Applicable Laws prohibit the furnishing of such information to the Data Controller. The Data Processor shall never process the Personal Data in a manner inconsistent with the Data Controller's documented instructions. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes Applicable Laws.

4.3 The Parties have entered into a Service Agreement in order to benefit from the expertise of the Processor in securing and processing the Personal Data for the purposes set out in Paragraph 3.1. The Data Processor shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements of this Addendum.

4.4 Data Controller warrants that it has all necessary rights to provide the Personal Data to Data Processor for the Processing to be performed in relation to the Services. To the extent required by Applicable Laws, Data Controller is responsible for ensuring that any necessary data subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Should such a consent be revoked by the data subject, Data Controller is responsible for communicating the fact of such revocation to the Data Processor, and Data Processor remains responsible for implementing any Data Controller instruction with respect to the further processing of that Personal Data.

**5. Confidentiality**

5.1 Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall treat all Personal Data as strictly confidential and it shall inform all its employees, agents and/or Sub-Processors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

**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, without prejudice to any other security standards agreed upon by the Parties, the Data Controller and Data Processor shall implement appropriate technical and organizational measures to ensure a level of security of the processing of Personal Data appropriate to the risk. These measures shall include as appropriate:

(a) measures to ensure that the Personal Data can be accessed only by authorized personnel for the purposes set forth in Paragraph 3.1 of this Addendum;
(b) in assessing the appropriate level of security account shall be taken in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of Personal Data;
(c) measures of pseudonymization and encryption of Personal Data;
(d) measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(e) measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of physical or technical incident;
(f) processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data;
(g) measures for user identification and authorization;
(h) measures for the protection of data during transmission;
(i) measures for the protection of data during storage;
(j) measures for ensuring physical security of locations at which Personal Data are processed;
(k) measures for ensuring events logging;
(l) measures for ensuring system configuration, including default configuration;
(m) measures for internal IT and IT security governance and management;
(n) measures for certification/assurance of processes and products;

(o) measures for ensuring data minimization;
(p) measures for ensuring data quality;
(q) measures for ensuring limited data retention;
(r) measures for ensuring accountability;
(s) measures for allowing data portability and ensuring erasure; and
(t) measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide services to the Data Controller.

**7. Improvements to Security**

7.1 The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Data Processor will therefore evaluate the measures as implemented in accordance with Paragraph 6.1 on an on-going basis and will tighten, supplement, and improve these measures in order to maintain compliance with the requirements set out in Paragraph 6.1. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in the Applicable Laws.

7.2 Where an amendment to the Service Agreement is necessary in order to execute a Data Controller instruction to the Data Processor, or to improve security measures as may be required by changes in the Applicable Laws from time to time, the Parties shall negotiate an amendment to the Service Agreement in good faith.

**8. Data Transfers**

8.1 Data Controller acknowledges and agrees that Data Processor may access and process and transfer Personal Data to provide the Services, including in the United States and to other countries where Data Processor and its Sub-Processors have operations. Where Personal Data is transferred outside of its country of origin, each Party will ensure that such transfers are made in compliance with all Applicable Laws.

8.2 To the extent that the Data Controller or the Data Processor are relying on a specific statutory mechanism to normalize international data transfers that is subsequently modified, revoke, or held in a court of competent jurisdiction to be invalid, the Data Controller and the Data Processor agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

**9. Information Obligations and Incident Management**

9.1 When the Data Processor becomes aware of an incident that impacts the Processing of the Personal Data that is the subject of the Service Agreement, it shall promptly notify the Data Controller about the incident, shall at all times cooperate with the Data Controller, and shall follow the Data Controller's instructions with regard to such incidents, in order to enable the Data Controller to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident.

9.2 The term "incident" used in Paragraph 9.1 shall be understood to mean in any case:

(a) a complaint or a request with respect to the exercise of a data subject's rights under Applicable Laws;
(b) an investigation into or seizure of the Personal Data by government officials, or a specific indication that such an investigation or seizure is imminent;
(c) any unauthorized or accidental access, processing, deletion, loss or any form of unlawful processing of the Personal Data;

(d) any breach of the security and/or confidentiality as set out in Paragraphs 5 and 6 of this Addendum leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data, or any indication of such breach having taken place or being about to take place;

(e) where, in the opinion of the Data Processor, implementing an instruction received from the Data Controller would violate Applicable Laws to which the Data Controller or the Data Processor are subject.

9.3 The Data Processor shall at all times have in place written procedures which enable it to promptly respond to the Data Controller about an incident. Where an incident is reasonably likely to require a data breach notification by the Data Controller under Applicable Laws, the Data Processor shall implement its written procedures in such a way that it is in a position to notify the Data Controller no later than 24 hours of having become aware of such an incident.

9.4 Any notifications made to the Data Controller pursuant to this Section shall be addressed to the data protection officer or other employee of the Data Controller whose contact details are provided during the registration process, and shall contain:

(a) a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) the name and contact details of the Data Processor's data protection officer or another contact point where more information can be obtained;

(c) a description of the likely consequences of the incident; and

(d) a description of the measures taken or proposed to be taken by the Data Processor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

**10. Contracting with Sub-Processors**

10.1 The Data Controller authorizes the Data Processor to engage the Sub-Processors further detailed in Annex I for the Service-related activities specified as described in Paragraph 3.1. Data Processor shall inform the Data Controller of any addition or replacement of such Sub-Processors at least 10 days in advance, thereby giving the Data Controller an opportunity to object to such changes.

10.2 Notwithstanding any authorization by the Data Controller with the meaning of the preceding paragraph, the Data Processor shall remain fully liable vis-à-vis the Data Controller for the performance of any such Sub-Processor that fails to fulfill its data protection obligations.

10.3 The Data Processor shall ensure that Sub-Processors are bound by the same data protection obligations of the Data Processor under this Addendum, shall supervise compliance thereof, and must in particular impose on its Sub-Processors the obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of Applicable Laws.

10.4 The Data Controller may request that the Data Processor audit a Sub-Processor or provide confirmation that such an audit has occurred (or, where available, obtain or assist customer in obtaining a third-party audit report concerning the Sub-Processor's operations) to ensure compliance with its obligations imposed by the Data Processor in conforming with this Addendum.

**11. Returning or Destruction of Personal Data**

11.1 Upon termination of the Service Agreement, upon the Data Controller's written request, or upon fulfillment of all purposes agreed in the context of the Services whereby no further processing is required, the Data Processor shall, at the discretion of the Data Controller, either delete, destroy, or return all Personal Data to the Data Controller and destroy or return any existing copies.

11.2 The Data Processor shall notify all third parties supporting its own processing of the Personal Data of the termination of the Service Agreement and shall ensure that all such third parties shall either destroy the Personal Data or return the Personal Data to the Data Controller, at the discretion of the Data Controller.

**12. Assistance to Data Controller**

12.1 The Data Processor shall assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Data Controller's obligation to respond to a request for exercising the data subject's rights under Applicable Laws.

12.2 The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to Paragraph 6 (Security), and shall make available to the Data Controller all information necessary to demonstrate compliance with the Data Processor's obligations and to allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

**13. Liability and Indemnity**

13.1 The Data Processor indemnifies the Data Controller and holds the Data Controller harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Controller and arising directly or indirectly out of or in connection with a breach of this Addendum and/or Applicable Laws by the Data Processor. The Data Controller indemnifies the Data Processor and holds the Data Processor harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Data Processor and arising directly or indirectly out of or in connection with a breach of this Addendum and/or Applicable Laws by the Data Controller.

**14. Duration and Termination**

14.1 This Addendum shall come into effect on the date the Data Controller signs this Addendum, which may be through electronic means.

14.2 Termination or expiration of the Service Agreement shall not discharge the Data Processor from its confidentiality obligations pursuant to Paragraph 5.

14.3 The Data Processor shall process Personal Data until the date of termination of the Service Agreement, unless instructed otherwise by the Data Controller, or until such data is returned or destroyed on instruction of the Data Controller.

**15. Miscellaneous**

15.1 In the event of any inconsistency between the provisions of this Addendum and the provisions of the Service Agreement, the provisions of this Addendum shall prevail.

This Agreement is executed by: )
)

_____ (Signature)

_____ (Print name)

_____ (Title)

_____ (DATE)

For and on behalf of

_____,

**Data Controller**

This Agreement is executed by: )
)

_____ (Signature)

_____ (Print name)

_____ (Title)

_____ (DATE)

For and on behalf of

**Hertza, L.L.C., dba ZeroBounce, Data Processor**

## ANNEX I:

### LIST OF SUB-PROCESSORS

The Data Controller has authorized the use of the Sub-Processors listed at:
https://www.zerobounce.net/docs/about-zerobounce/#subprocessors_and_service_providers/