EU DATA PROCESSING ADDENDUM

This EU 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**") and the company whose information has been provided as part of the registration process (hereinafter to be referred to as: the "**Data Controller**"). 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 that is subject to EU Data Protection Law 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 EU Data Protection Law shall mean 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, and repealing Directive 95/46/EC (General Data Protection Regulation).
    2.2 Terms such as "Processing", "Personal Data", "Data Controller", "Processor", and "data subject" shall have the meaning ascribed to them in the EU Data Protection Law.
    2.3 "Standard Contractual Clauses" shall, based on the circumstances unique to the Data Controller, mean the Standard Contractual Clauses (Controller to Processor) pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021, attached hereto as Exhibit A.

3. **Details of the Transfer**
    3.1 Insofar as the Data Processor will be processing Personal Data subject to EU Data Protection Law 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. **The Data Controller will transfer Personal Data to be processed by the Data Processor on computer servers located in the European Union. The**

categories of Personal Data to be processed includes: first name; last name; gender; city; state; country; Internet Protocol (IP) Address information; and email addresses. The types of data subjects whose information will be processed are individuals. The purposes for which the personal data will be processed include: validation of email lists for deliverability; removal of known email complainers, abusers and spam traps from email address lists; 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 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 that law explicitly prohibits 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 EU Data Protection Law or other Union or Member State data protection provisions.

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 Section 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 EU Data Protection Law, 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 approved 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 Section 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.

ZeroBounce takes the following security measures and those described in Annex II, to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access:

- All Personal Data received hereunder will be stored and processed in the EU;
- In addition to the above, while ZeroBounce does not rely on the EU-US and Swiss-US Privacy Shield Programs as a lawful basis for international transfers of personal information, ZeroBounce is an active participant in the EU-US and Swiss-US Privacy Shield Programs;
- ZeroBounce has restricted access to four personnel members with the ability to directly access files containing personal information on ZeroBounce servers, each of whom have agreed to maintain the confidentiality of any personal information;
- All data uploads and downloads sent between ZeroBounce and its customers flow through third party CloudFlare's servers in the EU;
- In addition to the above, while Cloudflare does not rely on the EU-US and Swiss-US Privacy Shield Programs as a lawful basis for international transfers of personal information, CloudFlare is an active participant in the EU-US Privacy Shield Program;
- The ZeroBounce support team does not have access to CloudFlare;
- CloudFlare maintains its own security protections to block threats and limit abusive bots and crawlers. See https://support.cloudflare.com/hc/en-us/articles/205177068-Step-1-How-does-Cloudflare-work-
- Any information that is uploaded by a ZeroBounce customer to ZeroBounce.net is transmitted via SSL through CloudFlare, and all files are stored in an encrypted file using a standard algorithm for protection of stored data defined by IEEE P1619 on ZeroBounce servers in the EU; and
- If customer elects to receive files via email, such files shall be sent encrypted, with a password via a separate email.

6.2 The Data Processor shall at all times have in place an appropriate written security policy with respect to the processing of Personal Data, outlining in any case the measures set forth in Paragraph 6.1.

6.3 At the request of the Data Controller, the Data Processor, shall demonstrate the measures it has taken and shall allow the Data Controller to audit and test such measures. The Data Controller shall be entitled on giving at least 14 days' notice to the Data Processor to carry out, or have carried out by a third party who has entered into a confidentiality agreement with the Data Processor, audits of the Data Processor's premises and operations as these relate to the Personal Data. The Data Processor shall cooperate with such audits carried out by or on behalf of the Data Controller and shall grant the Data Controller's auditors reasonable access to any premises and devices involved with the Processing of the Personal Data. The Data Processor shall provide the Data Controller and/or the Data Controller's auditors with access to any information relating to the Processing of the Personal Data as may be

reasonably required by the Data Controller to ascertain the Data Processor's compliance with this Addendum.

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 EU Data Protection Law or by data protection authorities of competent jurisdiction.

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 applicable data protection law from time to time, the Parties shall negotiate an amendment to the Service Agreement in good faith.

8. Data Transfers

8.1 The Data Processor shall not disclose Personal Data received hereunder to a third party or transfer it to a non-EU/European Economic Area (EEA) country without the Data Controller's authorization. The Data Processor shall immediately notify the Data Controller of any (planned) permanent or temporary transfers of Personal Data to a country outside of the EU/EAA without an adequate level of protection and shall only perform such a (planned) transfer after obtaining authorization from the Data Controller, which may be refused at its own discretion.

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 EU Data Protection Law;

(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 the EU Data Protection Law, 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 Article 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 sub-processors in the country locations 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 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 consent of the Data Controller pursuant to Paragraph 10.1 shall not alter the fact that consent is required for the engagement of sub-processors in a country outside the European Economic Area without a suitable level of protection.

10.4 The Data Processor shall ensure that the sub-processor is 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 EU Data Protection Law.

10.5 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 the GDPR.

12.2 The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to Paragraph 6 (Security) and prior consultations with supervisory authorities required under Article 36 of the GDPR taking into account the nature of processing and the information available to the Data Processor.

12.3 The Data Processor 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 the EU Data Protection Law 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 the EU Data Protection Law 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

EXHIBIT A: STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I. (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified herein.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Omitted

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex

II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least thirty days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance,

the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

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 Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor): controller/"Data Controller"

Data importer(s):

Name: Hertza L.L.C., dba ZeroBounce

Address: 10 E. Yanonali, St., Santa Barbara, CA 93101

Contact person's name, position and contact details: Vlad Cristescu, Head of Cyber Security, vlad.cristescu@zerobounce.net

Activities relevant to the data transferred under these Clauses: validation of email lists for deliverability; removal of known email complainers, abusers, and spam traps from email lists

Signature and date: _____

Role (controller/processor): processor/"Processor"

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Data Controller's customers who have consented to the processing of their personal data.

Categories of personal data transferred: personal data, address data, contact details, and technical data (may include first name, last name, gender, city, state, country, IP address, and email address).

Sensitive data transferred (if applicable) and applied restrictions or safeguards: not applicable.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Data Controller determines the frequency with which it transfers personal data (could be one-time, or could be multiple-times).

Nature of the processing: to provide Services to the Data Controller under the Service Agreement, which may include validation of email lists for deliverability; removal of known email complainers, abusers, and spam traps from email lists.

Purpose(s) of the data transfer and further processing: to receive Services under the Service Agreement, which may include validation of email lists for deliverability; removal of known email complainers, abusers, and spam traps from email lists.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: the earlier of: (i) expiration of thirty (30) days from receipt; (ii) the termination of the Service Agreement, or (iii) Data Controller's election to delete the personal data submitted to Processor.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: used in limited instances for duration of the Service Agreement, where Controller submits a request for support using our chat function/form, attaches an email list in conjunction with a request for support, or where improper use of our API occurs, resulting in the generation of an error log. Processing may include collection, storage, and retrieval.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: Ireland

---

ANNEX II

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

See Paragraph 6.1of the Addendum and the following details: ZeroBounce has implemented and shall maintain a security program in accordance with SOC2 Type II standards. ZeroBounce's security program includes the following technical and organizational security measures:

Measures of pseudonymization and encryption of Personal Data
ZeroBounce utilizes full disk encryption for all device that store Personal Data

ZeroBounce uses data hashing to anonymize cached data.
ZeroBounce encrypts customer validation data using customer unique keys.
ZeroBounce uses the latest industry best practices to ensure confidentiality through encryption of customer data both at rest and in transit, with the latest versions of TLS protocol and full disk encryption.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
Our data integrity is protected by Cloudflare's perimeter security and Bitdefender engine on the internal side, where we use anti-ransomware, anti-malware and antivirus artifacts. Daily backups and periodic testing of the backups ensure our own and our customer's data availability and resilience.

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
ZeroBounce's Business Continuity and Disaster Recovery plans and procedures form the foundation of our operational team's methods of ensuring the possibility of almost immediate recovery and restore of data from a secondary location, in case of a natural or technical disaster. In addition, ZeroBounce's full, differential or incremental backup procedures are set up so the data can be restored without issues in the fastest way possible.

Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data
ZeroBounce uses ISO, NIST and other industry known trusted sources for recommendations on how to implement its security controls. Being both ISO 27001 and SOC 2 Type II certified, we ensure that our code is built with security principles as foundation; we test it using world's top security researchers before deploying it on production servers and we contract top industry hackers to test all the missing bits, so that we can fix and improve continuously. Besides our state of the art proprietary algorithms, we keep track of all non-conformities or vulnerabilities found; we assign and keep track of rectifying such with high priority.

Measures for user identification and authorization
ZeroBounce is partnered with OKTA for customer identity management.

Measures for the protection of data during transmission
ZeroBounce utilizes end to end encryption for all data transmissions.

Measures for the protection of data during storage
ZeroBounce utilizes full disk encryption for all devices that store data.

Measures for ensuring physical security of locations at which Personal Data are processed
Access to our data centers is provided by state of the art access control systems that permit entry only to authorized personnel, following a strict schedule. All access is monitored and logged. Environmental conditions in our data centers are closely observed and ideal conditions are maintained by modern HVAC systems.

Measures for ensuring events logging
ZeroBounce systems log all relevant data access events.

Measures for internal IT and IT security governance and management
ZeroBounce has IT and IT Security governance policies and procedures that align with ISO 27001 and SOC Type2 standards. These include but are not limited to measures to categorize and mitigate risks, measure for threat and vulnerability analysis and mitigation, measures for data governance, measures for identity and role based access management.

Measures for certification/assurance of processes and products
ZeroBounce is ISO 27001 and SOC 2 Type II certified. We have a yearly accreditation plan for both certifications and we have a continuous improvement and monitoring system in place. This is done using ZeroBounce's Security and Compliance team and all the policies and procedures are re-evaluated on a yearly basis.

Measures for ensuring data minimization
ZeroBounce has data governance measures in place that ensure all data stored is adequate, relevant and limited to what is necessary for the validation and commercial process.

Measures for ensuring limited data retention
ZeroBounce utilizes a data retention policy that clearly defines data types, format, retention period, archiving and deletion process and procedures in the event of a violation.
ZeroBounce will not store single validation requests and output unless users opt in to "Help make Zerobounce better".
ZeroBounce will store files sent for validation for up to 30 days with the option granted to the user to delete files at will.
ZeroBounce has robust measures in place to deal with data erasure requests.

Measures for ensuring accountability
ZeroBounce enforces accountability through process ownership, so that each business process, service or division has a single owner who takes full responsibility and accountability.
ZeroBounce shall require its sub-processors to take appropriate technical and organizational measures to provide assistance to the controller and/or data exporter that are no less restrictive than those within the ZeroBounce Data Security Policy.

ANNEX III:

LIST OF SUB-PROCESSORS

The Data Controller has authorized the use of the following sub-processors:

1. Zendesk, Inc.

989 Market St.

San Francisco, CA 94103

Used in the limited instance where a customer submits a request for support using our chat function/form. Processing may include collection, storage, and retrieval.

2. Google

1600 Amphitheatre Parkway

Mountain View, CA 94043

Used in the limited instance where a customer attaches an email list in conjunction with a request for support. Processing may include collection and storage.

3. Cloudflare, Inc.

101 Townsend St.

San Francisco, CA 94107

Used in the limited instance where improper use of our API occurs, resulting in the generation of an error log (e.g., connection is from a banned location, or too many connections were attempted in a short timespan triggering a rate limit). Processing may include collection and storage.