UK DATA PROCESSING ADDENDUM

This UK 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 "**Importer**") and the company whose information has been provided as part of the registration process (hereinafter to be referred to as: the "**Exporter**"). Importer and Exporter 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 Addendum**
    1.1 This Addendum applies exclusively to the processing of personal data that is subject to the UK GDPR 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**"). The parties would like to rely on the European Commission's Standard Contractual Clauses for international data transfers adopted by European Decision 914/2021/EU ("EU SCC"), and the UK International Data Protection Addendum for the transfer of personal data from the UK.

2. **Definitions**
    2.1 "UK GDPR" 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 (United Kingdom General Data Protection Regulation), tailored by the Data Protection Act 2018.
    2.2 "Applicable Data Protection Law" means the data protection law of the UK which is the UK GDPR and the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended), and other data protection or privacy legislation in force from time to time in the United Kingdom;
    2.3 Terms such as "Personal Data", "Special Categories of Data", "Process/Processing", "Exporter", "Importer", "data subject", "sub-processor," and "technical and organisational security measures" shall have the same meaning ascribed to them in the UK GDPR.
    2.4 "Standard Contractual Clauses" shall, based on the circumstances unique to the Exporter, mean the International Data Transfer Addendum to the EU Commission SCCs, promulgated by the IOC, attached hereto as Exhibit A.

3. Details of the Transfer

3.1 Insofar as the Importer will be processing Personal Data subject to the UK GDPR on behalf of the Exporter in the course of the performance of the Service Agreement with the Exporter the terms of this Addendum shall apply. **The Exporter will transfer Personal Data to be processed by the Importer on computer servers located in the European Union.**

4. The Exporter and the Importer

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

4.2 The Importer will only process the Personal Data on documented instructions of the Exporter 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 Importer is subject. In such a case, the Importer shall inform the Exporter of that legal obligation before processing, unless that law explicitly prohibits the furnishing of such information to the Exporter. The Importer shall never process the Personal Data in a manner inconsistent with the Exporter's documented instructions. The Importer shall immediately inform the Exporter if, in its opinion, an instruction infringes the UK GDPR.

4.3 The Parties have entered into a Service Agreement in order to benefit from the expertise of the Importer in securing and processing the Personal Data for the purposes set out in Section 3.1 above. The Importer 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 Exporter warrants that it has all necessary rights to provide the Personal Data to Importer for the Processing to be performed in relation to the Services. To the extent required by the UK GDPR, Exporter 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, Exporter is responsible for communicating the fact of such revocation to the Importer, and Importer remains responsible for implementing any Exporter 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 Importer 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 Importer 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 Exporter and Importer 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 Exporter.

ZeroBounce takes the following security measures and those described in Appendix 2, 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 protections to block threats and limit abusive bots and crawlers. See https://support.cloudflare.com/hc/en-us/articles/ security 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 Importer 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 Exporter, the Importer, shall demonstrate the measures it has taken and shall allow the Exporter to audit and test such measures. The Exporter shall be entitled on giving at least 14 days notice to the Importer to carry out, or have carried out by a third party who has entered into a confidentiality agreement with the Importer, audits of the Importer's premises and operations as these relate to the Personal Data. The Importer shall cooperate with such audits carried out by or on behalf of the Exporter and shall grant the Exporter's auditors reasonable access to any premises and devices involved with the Processing of the Personal Data. The Importer shall provide the Exporter and/or the Exporter's auditors with access to any information relating to the Processing of the Personal Data as may be reasonably required by the Exporter to ascertain the Importer'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 Importer 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 UK GDPR or by data protection authorities of competent jurisdiction.

7.2 Where an amendment to the Service Agreement is necessary in order to execute an Exporter instruction to the Importer, 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 For the Services, Exporter will transfer Personal Data to be processed by the Importer on computer servers located in the EU. The Importer 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 Exporter's authorization. The Importer shall immediately notify the Exporter 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 Exporter, which may be refused at its own discretion.

8.2 To the extent that the Exporter or the Importer 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 Exporter and the Importer 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 Importer 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 Exporter about the incident, shall at all times cooperate with the Exporter, and shall follow the Exporter's instructions with regard

to such incidents, in order to enable the Exporter 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 the UK GDPR;

(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 Importer, implementing an instruction received from the Exporter would violate applicable laws to which the Exporter or the Importer are subject.

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

9.4 Any notifications made to the Exporter pursuant to this Article shall be addressed to the Data Protection Officer or other employee of the Exporter 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 Importer'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 Importer to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

10. Contracting with Sub-Processors

10.1 The Exporter authorizes the Importer to engage sub-processors in the country locations for the Service-related activities specified as described in Paragraph 3.1. Importer shall inform the Exporter of any addition or replacement of such sub-processors giving the Exporter an opportunity to object to such changes.

10.2 Notwithstanding any authorization by the Exporter with the meaning of the preceding paragraph, the Importer shall remain fully liable vis-à-vis the Exporter for the performance of any such sub-processor that fails to fulfill its data protection obligations.

10.3 The consent of the Exporter 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 Importer shall ensure that the sub-processor is bound by the same data protection obligations of the Importer 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 the UK GDPR.

10.5 The Exporter may request that the Importer 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 Importer in conforming with this Addendum.

11. Returning or Destruction of Personal Data

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

11.2 The Importer 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 Exporter, at the discretion of the Exporter.

12. Assistance to Exporter

12.1 The Importer shall assist the Exporter by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Exporter's obligation to respond to a request for exercising the data subject's rights under the UK GDPR.

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

12.3 The Importer shall make available to the Exporter all information necessary to demonstrate compliance with the Importer's obligations and to allow for and contribute to audits, including inspections, conducted by the Exporter or another auditor mandated by the Exporter.

13. Liability and Indemnity

13.1 The Importer indemnifies the Exporter and holds the Exporter harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Exporter and arising directly or indirectly out of or in connection with a breach of this Addendum and/or the UK GDPR by the Importer. The Exporter indemnifies the Importer and holds the Importer harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Importer and arising directly or indirectly out of or in connection with a breach of this Addendum and/or the UK GDPR by the Exporter.

14. Duration and Termination

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

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

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

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

_____, Exporter

This Agreement is executed by:)
)

_____ (Signature)

_____ (Print name)

_____ (Title)

_____ (DATE)

For and on behalf of

Hertza, L.L.C., dba ZeroBounce, Importer

EXHIBIT A: INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES[1]

Part 1: Tables

Table 1: Parties

Start date	Effective date of the Service Agreement between Importer and Exporter	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name and contact details: Customer, as noted in the Service Agreement	Full legal name and contact details: Supplier, as noted in the Service Agreement
Key Contact	As noted in the Service Agreement	As noted in the Service Agreement

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	**Module in operation**	**Clause 7 (Docking Clause)**	**Clause 11 (Option)**	**Clause 9a (Prior Authorisation or**	**Clause 9a (Time period)**	**Is personal data received from the Importer**

[1] Version B1.0, in force March 2022

				General Authorisation)		**combined with personal data collected by the Exporter?**
	2	**N/A**	**N/A**	**General Written Authorisation**	**As set out in the Service Agreement**	**No**

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:

Exporter:

Name: Customer as noted in the Service Agreement

Address: Customer's address as noted in the Service Agreement

Contact person's name, position, and contact details: Customer's contact details as noted in the Service Agreement

Activities relevant to the data transferred under these Clauses: processing of personal data in connection with Customer's use of the agreed upon Services

Importer:
Name: Provider as noted in the Service Agreement

Address: Provider's address as noted in the Service Agreement

Contact person's name, position, and contact details: Provider's contact details as noted in the Service Agreement

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 address lists; to perform any additional services requested by Customer/Exporter

Importer's representative in the European Union: Vlad Cristescu

Importer's representative in the European Union email address: vlad.cristescu@zerobounce.net; gdpr@zerobounce.net

Importer's representative in the UK: Vlad Cristescu

Importer's Data Protection Officer's email address: vlad.cristescu@zerobounce.net; gdpr@zerobounce.net

Role (controller/processor): processor

Annex 1B: Description of Transfer:

Categories of data subjects whose personal data is transferred:
Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects: Customer's prospects, customers, business partners and vendors

Categories of personal data transferred:
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.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: The parties do not anticipate the transfer of sensitive data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):
Continuous basis.

Nature of the processing:
Importer will process personal data as necessary to perform the services and as further instructed by Exporter in its use of the Services.

Purpose(s) of the data transfer and further processing:
Performance of the agreed upon Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:
Importer will process personal data for the duration of the Service Agreement, in accordance with the data storage procedures and timeframes set out in the Service Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:
Personal data may be transferred to (sub-) processors for performance of the Services, as further instructed by Importer in its use of the Services. (Sub-) processors will process personal data for

the duration of the Service Agreement, in accordance with the data storage procedures and timeframes set out in the Service Agreement.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

The following technical and organizational measures are performed on the processes taken by Importer:

Please refer to the description of the Importer's security measures set out in Paragraph 6.1 of the Addendum. Importer has implemented and shall maintain a security program in accordance with SOC2 Type II standards. Importer'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 the 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 Importer and/or Exporter that are no less restrictive than those within the ZeroBounce Data Security Policy

Annex III: List of Sub processors (Modules 2 and 3 only): The list below contains the third-party Sub-Processors that are currently relied upon by Supplier in connection with the Services and may be used in connection with Supplier's Processing of Customer Data.

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.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	**Which Parties may end this Addendum as set out in Section 19:** ☒ **Importer** ☒ **Exporter** ☐ **neither Party**

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.

Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the Exporter to the Importer, to the extent that UK Data Protection Laws apply to the Exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "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";

c. Clause 6 (Description of the transfer(s)) is replaced with:

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

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

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

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a. its direct costs of performing its obligations under the Addendum; and/or
b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.