BOOMERANG
Customer Data Processing Addendum for Self-Serve Portal Subscription Plan

This Data Processing Addendum (hereinafter referred to as the "Data Processing Addendum" or "Addendum) forms an integral part of the Self-Serve Portal Subscription Plan agreement (the "Agreement") between Thanks Boomerang, Inc., (the "Provider") and between the counterparty agreeing to these terms (the "Customer") and applies to the extent the Provider processes Personal Data on behalf of the Customer, in the course of its performance of its obligations under the Agreement. By accepting the Agreement the Customer accepts the terms in this Addendum.

1. General Definitions. All capitalized terms not otherwise defined herein shall have the meanings set forth in the Agreement.

2. Scope of Addendum. As of the Agreement Effective Date and for any period of time thereafter during which Provider is a data importer and has possession of or access to Customer Personal Data in connection with the Services until expiration or termination of the Agreement, Provider shall have implemented at its Facilities, and shall thereafter maintain policies, procedures and practices that satisfy the applicable requirements set forth in this Data Processing Addendum. Additionally, at all times during the duration of the Agreement and for any period of time thereafter during which Provider is a data importer and has possession of or access to Customer Personal Data in connection with the Services, Provider shall maintain compliance with all applicable Data Protection Laws. Notwithstanding the foregoing, if Provider cannot provide such compliance for whatever reasons, it agrees to promptly inform Customer of its inability to comply, in which case the Customer is entitled to suspend the transfer of Personal Data.

3. Data Processing/Privacy Definitions. For purposes of this Data Processing Addendum, the words "Controller", "Data Subject", "Member State", "Personal Data", "Process", "Processor" and "Processing" will have the meaning given to these terms in accordance with the applicable country-specific Data Protection Laws, including but not limited to, the EU General Data Protection Directive (GDPR) (or where not defined in applicable Data Protection Laws, will have the meaning as in UK Data Protection Laws). During the term of the Agreement:

   "Customer Personal Data" means the Personal Data about Customer and its personnel that Provider receives from Customer, or otherwise Processes for or on behalf of Customer in order to provide the Services (including any products) under the Agreement.

   "Data Protection Laws" means any law covering "Personal Data", "Process(ing)" and "Data Subject(s)", including the GDPR, UK Data Protection Laws, and all other country's privacy laws, including Member State's data protection laws and regulations applicable to Provider as a data importer of Customer Personal Data in the performance of the Services under the Agreement.

   "Facilities" or "Facility" means the Provider's facility(s) used now or in the future to perform the Services pursuant to the Agreement that have access to, store, Process or use Customer Personal Data.

   "Member State" means a country that is a member of the European Union or the European Economic Area.

"Personal Data Breach" shall mean a breach of Data Protection Laws and any personal data breach as defined in such Data Protection Laws;

“Personnel” means all workers, including but not limited to Provider’s employees, temporary personnel, and others employed or contracted by Provider that have access, store, Process or use Customer Personal Data.

Service(s) means the services provided by Provider pursuant to the Agreement.

“Subcontractor” means Provider’s vendors, agents, subcontractors, and all other persons, entities, or organizations, exclusive of non-contingent Customer employees who are subject to the direction, supervision, and control of Provider.

“Sub-processor” means any Subcontractor engaged by Provider to Process Customer Personal Data who are identified in Appendix 1 of this Addendum.

"UK Data Protection Laws" means the “UK GDPR” as defined in the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations (each as amended from time to time) and other data protection or privacy legislation in force from time to time in the United Kingdom.

4. Processing. In performing its obligations in the Agreement, if Provider at any time from the Agreement Effective Date and until termination of the Services or the Agreement undertakes Processing of Personal Data for or on behalf of Customer, Provider will process all Personal Data fairly and lawfully, respecting the Data Subject's privacy, and in accordance with all Data Protection Laws applicable to such Processing of Personal Data. Provider will take reasonable measures to require that all of its Personnel and each of its Sub-processors process all Personal Data in a similar manner as further described in Section 5 below. Provider will only Process Customer Personal Data for the purposes of and in compliance with the terms set out in the Agreement or this Data Processing Addendum and in compliance with mutually agreed Customer's instructions as issued from time to time. Provider will not *(i)* obtain any rights to any Personal Data by virtue of complying with its obligations in the Agreement and/or this Addendum; *(ii)* except with respect to approved Sub-processors or pursuant to applicable law, transfer or disclose any Personal Data (in part or in whole) to any third party, except as stipulated in this Data Processing Addendum, *(iii)* except as technically necessary to perform its obligations under the Agreement, transfer, access or store any Personal Data outside of the country in which the applicable Provider Facility is established (the “Country Of Origination”), including via cloud services, without the explicit prior consent of Customer, or (*iv*) Process or use any Personal Data for its own purposes or benefit. Provider will keep all Personal Data confidential and secure.

5. Third Parties & Sub-processors. Provider may subcontract its processing work that relates to Personal Data under the Agreement only with prior written consent of Customer. Additionally, Provider must provide a list of current Sub-processors under Appendix 1 of this Addendum. Such sub-processor list shall include the identities of those Sub-processors and their country of location and have been consented to by Customer. If Provider decides at a later date to use Sub-processors, Provider must inform Customer in writing. Provider must inform Customer prior to any changes or replacements of Sub-processors and request Customer’s explicit approval for such change. Customer shall not unreasonably object to such changes or replacements. If Provider is authorized by Customer to subcontract to a third party any of its performance obligations under the Agreement with respect to Processing Customer Personal Data, Provider shall require that its Sub-processors

also maintain adequate measures (reasonably appropriate to such subcontractor's storage, maintenance or processing activities) that comply in all material respects with the relevant obligations in this Addendum, including, but not limited to, the obligations of data privacy, confidentiality, information security and international transfers. Subject to the limitations set forth herein and in Section 13 of the Agreement, to the extent caused by Provider will be held accountable and liable to Customer for any Personal Data privacy violations or security breaches within the Service scope, to the extent caused by Provider's breach of its obligations under this Addendum.

6. International Transfers. All transfers of Customer Personal Data outside of the Country Of Origination by Provider (if any) will be in strict compliance with the relevant provisions of the Data Protection Laws in the originating country. Where the Personal Data originates in the EU or UK, transfers can only occur either to a country with adequate Data Protection Laws or pursuant to Privacy Shield, the EU Standard Contractual Clauses (including the UK Addendum, if applicable), or Binding Corporate Rules. All transfers of Personal Data by Provider not technically necessary to perform its obligations under the Agreement will be done with the prior written consent of Customer and will be made in strict accordance with applicable Data Protection Laws or contractual obligations on such transfers provided such contractual obligations do not violate applicable Data Protection Laws. All transfers of Personal Data outside of Canada, or countries within Asia Pacific and Latin America will be done so in accordance with applicable Data Protection Laws.

7. Cooperation & Enquiries. Provider will inform Customer without undue delay if Provider receives any enquiry, complaint or claim from any court, governmental official, third parties or individuals (including but not limited to the Data Subjects) arising out of the Services and will provide Customer reasonable support and cooperation in a timely manner in responding to any such request. Should Customer, on the basis of applicable law, be obliged to provide access or information to a Data Subject about the Processing of Personal Data relating to him or her, Provider will, without levying a fee, reasonably assist Customer in providing such access or information.

8. Confidentiality & Information Security. In addition to any other agreement and/or terms governing confidentiality between the parties, Provider will adopt adequate (taking into account the nature of Processing and the information available to Provider) technical and organizational measures reasonably necessary to secure the Personal Data and to prevent unauthorized access, alteration or loss of the same, including measures required by applicable Data Protection Laws. Provider will also ensure confidentiality of the Personal Data, including taking appropriate measures to ensure the same of its Personnel and Sub-processors. At the reasonable written request of Customer, Provider will provide the former with a comprehensive and up-to-date data protection and security concept for the Customer Personal Data obtained under the Agreement while performing the Services under the Agreement.

9. Privacy Violations, Security and Data Breach Incidents. When known or reasonably suspected by Provider while performing the Services under the Agreement, Provider will inform Customer promptly if: (*i)* Provider or its Personnel infringe the applicable Data Protection Laws or obligations under the Agreement, *(ii)* significant failures during the Processing occur, or *(iii)* third parties have unauthorized or unintended access to the Personal Data. The parties are aware that the applicable Data Protection Law may impose a duty to inform the competent authorities or affected Data Subjects in the event of the loss or unlawful disclosure of Personal Data or access to it. These incidents should therefore be notified by Provider to Customer without delay, regardless of their origin. This also applies to serious operational faults or where there is any suspicion of an infringement of provisions relating to the protection of Personal Data or other irregularities in the handling of Personal Data belonging to Customer. In consultation with Customer, Provider must take appropriate measures, within the Service scope, to address the Personal Data Breach,

including, where appropriate, measures to secure the Personal Data and work in good faith to reduce risk to the Data Subjects whose Personal Data was involved. Provider must coordinate the messaging related to any privacy violation, security breach or data breach incident with the Customer prior to making any public disclosures.

10. Inspection & Audit Rights. Upon at least 30 days prior written notice and subject to the obligations herein, Customer may inspect Provider's operating Facilities or conduct an audit (each an "Audit"), Provider's security, quality processes and environmental systems controls used for processing Customer Personal Data to ascertain compliance with this Data Processing Addendum at Customer's expense (although Customer shall in no way be responsible for any expenses or costs incurred by Provider's commercially reasonable support in assisting Customer with the Audit or allowing Customer to inspect their Facilities, and in the event a violation of Provider's obligations under this Addendum is found that has the potential to compromise Customer Personal Data, Provider shall be responsible for all reasonable costs and expenses incurred by Customer in conducting the Audit). To the extent applicable to Provider's obligations under this Addendum, this Audit may include, but is not limited to, the verification of whether the procedures for the technical and organizational requirements of data protection and information security are appropriate in accordance with obligations negotiated by the parties either in an agreement and/or separate amendment/addendum. Provider will provide Customer with any reasonably necessary information and documents during the Audit. The Audit may be carried out once a year by Customer's data protection officer or a mutually accepted authorized representative unless a violation of Provider's obligations under this Data Processing Addendum is found, and in such an event, Customer may conduct another Audit within six months or if Customer reasonably believes that Provider is not complying with the obligations contained in this Addendum. All Audits will be performed during normal working hours; subject to Provider's reasonable security, safety, and confidentiality requirements; and in such a way that the Audit does not disrupt or compromise Provider's infrastructure or ability to process normal business operations. In addition, Provider will reasonably allow and assist in the Audit of its obligations (at its own expense) under this Addendum. In addition, Provider will cooperate with any audit ordered by a relevant Data Protection Authority that arises from its performance under the Agreement.

Notwithstanding the forgoing, any Audit, shall not entitle Customer to view, or in any way access records and/or processes:

i. Not directly related to Customer Data Processed by Provider;
ii. Not directly related to the Services provided to Customer under the Agreement;
iii. In violation of applicable laws; and/or
iv. In violation of Provider's confidentiality obligations owed to a third party

For clarity, Audits will only be performed if the parties have mutually agreed in writing on the scope of the Audit prior to any Audit. Customer will provide prior written notice, including a written explanation of the reason for the Audit, to the Provider no later than 30 days before any such Audit commences. Prior to any Audit, both parties shall agree to pursue, in good faith, other means of reconciling the documents that would render such Audits not necessary. The mutually accepted third party auditor will sign Provider's standard, confidential disclosure agreement, which will limit the third party auditor's rights to disclose to Customer anything other than the results of Provider's compliance or non-compliance with the Audit. Audit costs and expenses shall be mutually agreed upon between the parties in writing prior to any Audit.

11. Indemnity. Subject to the remaining provisions of this Section 11, the parties hereby agree that Provider shall have the obligation of defense and indemnification for any Claim incurred by or assessed against any Customer Indemnitee by third party for any willful or negligent acts or omissions by Provider or any violation of this Addendum or the Data Protection Laws but to the extent such violation has been caused by the Provider's willful or negligent acts or omissions while Processing Customer Personal Data as a data importer under this Addendum.

Notwithstanding anything contained in the Agreement, this Addendum or any other amendment or addendum, the parties agree (i) that if one party is held liable for a violation of the Data Protection Laws committed by the other party, the latter will, to the extent to which it is liable, indemnify the other party for any cost, charge, damages, expenses or loss it has incurred as part of its obligations to indemnify under Section 5, as applicable; and (ii) the limitations and exceptions in Section 7 (Limitations of Liability) of the Agreement, including Provider's total liability cap, applies to this Section 11.

The non-indemnifying party shall:

(i) promptly notify the other party upon learning of a Claim; and
(ii) cooperate in the defense and settlement of the Claim.

12. Return of Personal Data. Following termination of the Agreement, Provider, except to the extent prohibited by applicable law, at the sole discretion and written request of Customer, will return to Customer or destroy and delete all Customer Personal Data subject to Processing. Provider must certify in writing to Customer that it has complied with the foregoing obligations.

13. Counterparts. This Addendum may be executed in counterparts, each of which when executed and delivered shall constitute an original of the Addendum, but all the counterparts shall together constitute the same document. No counterpart shall be effective until each party has executed at least one counterpart. Facsimile or electronic signatures shall be binding to the same extent as original signatures.

14. Integration. Except as otherwise set forth in this Addendum, all terms and conditions contained in the Agreement shall remain in full force and effect. In the event of a conflict between the Agreement and this Addendum or any other confidentiality term in an agreement between the parties, the order of precedence in respect of the Processing of Customer Personal Data shall be: this Addendum and then the Agreement.

Appendix 1 to the Addendum
List of Agreed Sub-processors

Name of Sub-processor	Nature of Processing	Country Location of Sub-processor
Stripe	Customer billing data (name, credit, card, postal code)	USA
Mailgun (Sinch)	Address data (name, email address)	USA
Hubspot	Contact data (name, email address, phone number)	USA
Shippo	Mailing address data (name, address, phone number)	USA
Sentry	Customer data logging (name, email address, phone number)	USA