EASYPOST DATA PROCESSING ADDENDUM

This DATA PROCESSING ADDENDUM ("**DPA**") forms part of the Terms (the "**Agreement**") between Simpler Postage, Inc. (d/b/a EasyPost) ("**Company**") and Customer. Company and Customer will be referred to as a "Party" or collectively, as the "Parties" herein. This DPA shall be effective as of the date of the last signature below.

The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. If the terms of this DPA conflict with the Agreement, the Agreement will prevail to the extent of any conflict.

1. **Definition.** In this DPA, the following terms shall have the meanings set out below:
    1. "**Affiliate"** means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.
    2. "**Data Breach**" means a breach of security of Company's systems leading to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, access to, or other Processing of Personal Data transmitted, stored, or otherwise Processed on behalf of Customer.
    3. "**Data Protection Laws**" means all data protection laws and regulations applicable to a Party's Processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Laws and US Data Protection Laws.
    4. "**Data Subject Request**" means a request made by an End User in accordance with the rights granted under Data Protection Laws, including but not limited to requests to know, correct, delete and opt-out under US Data Protection Laws and requests to access, rectify, erase, restrict Processing, data portability, object to Processing and not to be subject to automated individual decision making under EU Data Protection Laws.
    5. **"End User"** means an individual user of Customer's Application(s) as set out in Annex A whose information is received from or on behalf of Customer.
    6. **"EU Data Protection Laws"** means all data protection laws and regulations applicable to Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council 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) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii);

(iv) in respect of the United Kingdom ("UK") any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the European Union) and (v) in respect of Switzerland, the Federal Act on Data Protection of 19 June 1992 ("FADP").

7. **"Europe"** means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

- 1. "**EU Standard Contractual Clauses**" means the contractual clauses set out in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council specifically including Module 2 (Controller to Processor).

2. "**Personal Data**" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable natural person or particular household received from or on behalf of Customer about Customer's End Users as set out in Annex A.

3. "**Process**" or "**Processing**" means any operation or set of operations which is performed on Personal Data by Company or its Subprocessors, or in connection with and for the purposes of the provision of the Services, whether or not accomplished by automatic means, including but not limited to collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; and as defined by Data Protection Laws.

4. "**Processor to Processor Clauses**" means, as relevant, (i) in respect of transfers of Personal Data subject to the GDPR, the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021 specifically including Module 3 (Processor to Processor) ; (ii) in respect of transfers of Personal Data subject to the U.K. GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner, in each case as amended, updated or replaced from time to time.

5. "**Sensitive Data**" means (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, credit, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, information about sexual life or sexual orientation, or criminal record; (e) account passwords; or (f) other information that falls within the definition of "special categories of data,", "special personal information," "sensitive personal information," or "sensitive data" under applicable Data Protection Laws.

6. "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Company for Customer pursuant to the Agreement.

7. "**Subprocessor**" means any person appointed by or on behalf of Company to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement. Subprocessors may include third parties or Affiliates of Company but shall exclude Company employees, contractors, or consultants.

8. "**Third Country**" means in relation to Personal Data transfers subject to the GDPR, any country outside of the scope of the data protection laws of the European Economic Area, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time; and (ii) in relation to Personal Data transfers subject to the U.K. GDPR, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing adequate protection for Personal Data by the relevant competent authority of the UK from time to time.

9. "**U.K. GDPR**" means 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) (United Kingdom General Data Protection Regulation), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (and see section 205(4)).

10. "**U.K. Standard Contractual Clauses**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner, as amended, updated or replaced from time to time.

11. "**US Data Protection Laws**" means the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA"), the Virginia Consumer Data Protection Act ("VCDPA"), the Colorado Privacy Act ("CPA"), the Utah Consumer Privacy Act ("UCPA") the Connecticut Act Concerning Personal Data Privacy and Online Monitoring ("CTDPA") and other similar comprehensive US state privacy laws that place obligations on a Business or Controller in relation to Personal Data, and any relevant regulation, rule, or other binding instrument which implements such laws.

12. The terms "**Data Subject**", and "**Supervisory Authority**" shall have the same meaning as in the EU Data Protection Laws and the terms "**Business**", "**Controller**", "**Processor**" and "**Service Provider**" shall have the same meanings as in the Data Protection Laws, as applicable.

1. **Processing of Personal Data.**
    1. **Roles of the Parties.** The parties acknowledge and agree that with respect to the Processing of Personal Data under the Agreement, Customer is the Business or Controller, and Company is the Processor or Service Provider. The subject matter, duration, purpose of the Processing, and types of Personal Data and categories of Data Subjects subject to this DPA are set forth in Annex A.

2. **Customer Obligations.** Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its Processing of Personal Data and any processing instructions it issues to Company; and (ii) it has provided, and will continue to provide, all notices and has obtained, and will continue to obtain, all consents and rights necessary under applicable Data Protection Laws for Company to Process Personal Data for the purposes described in the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Without prejudice to the generality of the foregoing, Customer agrees that it shall be responsible for complying with all laws (including Data Protection Laws) applicable to any content created, sent or managed through the Service.

3. **Company's Obligations.** Company will comply with Data Protection Laws applicable to its Processing of Personal Data to provide the Services. Company will Process Personal Data only in accordance with Customer's documented written instructions and as permitted in accordance with the Agreement. The Parties agree that the Agreement sets out Customer's complete and final instructions to Company in relation to the Processing of Personal Data, and processing outside of the scope of these instructions (if any) shall require prior written agreement of both of the Parties.

4. **Lawfulness of Customer's Instructions**. Customer shall ensure that Company's processing of Personal Data in accordance with Customer's instructions will not cause Company to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws.

5. **Third-Party Carriers.** To the extent Customer instructs Company to provide Personal Data to any third-party carrier, Customer understands and agrees that Company is unable to make representations regarding the applicable carrier, such carrier's systems, or such carrier's security measures, and Company shall not be responsible for any damages, liabilities, or claims resulting from or caused by any carrier or the carrier's systems. Customer shall be responsible for ensuring whether the security measures adopted by the applicable third-party carriers adequately meet its obligations under applicable Data Protection Laws.

2. **Subprocessing.**
    1. **General Authorization.** Customer generally authorizes the use of Subprocessors to Process Personal Data in connection with fulfilling Company's obligations under the Agreement and/or this DPA. A list of current Subprocessors can be viewed at Annex D (the "**Subprocessor List**"). Customer hereby authorizes Company to engage the Subprocessors listed in the Subprocessor List. For the avoidance of doubt, to the extent Customer instructs Company to provide Personal Data to any third-party carriers, such carriers are not Subprocessors as defined herein.

    2. **Communication With Subprocessors.** Customer shall not directly communicate with Company's Subprocessors about the Services, unless agreed to in writing by Company in

Company's sole discretion.

3. **Security.**
    1. **Company's Personnel**. Company shall ensure that any person who is authorized by Company to process Personal Data (including its staff and agents) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).
    2. **Security Measures.** Company shall implement and maintain commercially reasonable technical and organizational measures that are designed to protect against Data Breaches involving, and unauthorized or accidental destruction, loss, alteration or damage, unauthorized disclosure of or access to, Personal Data and designed to preserve the security and confidentiality of Personal Data, 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. For the avoidance of doubt, to the extent Customer instructs Company to provide Personal Data to any third-party carriers, Company is not able to represent or certify that such carriers' systems or that such carriers comply with these security measures.
    3. **Updates to Security Measures.** Customer acknowledges that the security measures are subject to technical progress and development and that Company may update or modify the security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services provides to Customer.
    4. **Customer's Obligations Regarding Security Measures.** Customer is responsible for independently determining whether the security measures adequately meet its obligations under applicable Data Protection Laws. Customer is also responsible for its secure use of the Services, including protecting the security of Personal Data in transit to and from the Services (including securely backing up or encrypting any such Personal Data).
4. **Data Breach.**
    1. **Notification.** In the event that Company becomes reasonably aware of any Data Breach, Company will use good faith efforts to notify Customer of the Data Breach without undue delay, but in no event later than five (5) business days after Company becomes reasonably aware of the Data Breach. The notification obligations in this Section 5 do not apply to incidents that are caused by Customer or Customer's personnel or users or to unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewall or networked systems.
    2. **Manner of Notification.** Notification of a Data Breach, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means that Company selects, including via electronic mail. It is Customer's sole responsibility to ensure that it maintains accurate contact information with Company at all times.

3. **Data Breach Management**. Company shall make commercially reasonable efforts to identify the cause of a Data Breach and take those steps that Company deems necessary and reasonable to remediate the cause of such Data Breach to the extent that remediation is within Company's reasonable control.

5. **Termination.**
    1. **Termination.** This DPA shall terminate automatically upon the later of (a) the termination or expiration of the Agreement; or (b) Company's deletion or return of the Personal Data to Customer.

    2. **Return or Deletion of Data**. Upon termination or expiration of this DPA, Company shall (at Customer's election) delete or return to Customer all existing copies of Personal Data, unless Data Protection Laws require continued retention of the Personal Data. Upon Customer's request, Company shall confirm compliance with these obligations in writing. Notwithstanding the foregoing, Company shall not be required to delete such Personal Data to the extent Company is required to retain such Personal Information in accordance with any applicable third-party carrier's requirements or to complete the Services for or on behalf of such Customer's End User. This requirement shall not apply to Personal Data that Company has archived on backup systems, which Personal Data shall be deleted by Company at such time as Company next restores to its active systems the backup that contains the Personal Data.

6. **Data Subject Requests.**
    1. **Data Subject Requests**. In the event that a Data Subject Request is made to Company, Company shall not respond to the Data Subject Request directly, except to direct the Data Subject to contact Customer directly or as required by Data Protection Laws. If Company is required by Data Protection Laws to respond to the Data Subject Request, it shall notify Customer by any means that Company selects, including via electronic mail, unless prohibited from doing so by Data Protection Laws. For the avoidance of doubt, nothing in the Agreement or the DPA shall restrict or prevent Company from responding to any Data Subject Request or request or inquiry from a Data Protection Authority in relation to Personal Data for which Company is a Controller.

7. **Jurisdiction Specific Terms.**
    1. To the extent that Company Processes Personal Data subject to EU Data Protection Laws, the terms of Annex B shall apply and are hereby incorporated into the DPA by this reference. To the extent that Company Processes Personal Data subject to US Data Protection Laws, the terms of Annex C shall apply and are hereby incorporated into the DPA by this reference.

8. **Limitation of Liability.**
    1. **Limitation of Liability.** To the extent permitted by applicable Data Protection Laws, each Party's (and all of that Party's Affiliates') liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) shall be subject to the exclusions and limitations of liability set forth in the Agreement.

2. **Claims by Customer.** Any claims made against Company or its Affiliates under or in connection with this DPA (including, where applicable, the SCCs) shall be brought solely by the Customer entity that is a party to the Agreement.

3. **Exclusion.** In no event shall any Party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

9. **General Provisions.**
    1. **Amendments**. Company reserves the right to amend, supplement, or update this DPA upon notice to Customer in order to comply with any requirements set forth in the applicable Data Protection Laws. This DPA may not otherwise be amended or supplemented, nor shall any of its provisions be deemed to be waived or otherwise modified, except through a writing duly executed by authorized representatives of Company and Customer.

    2. **Severability**. Should any provision of this DPA or any of the Annexes be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained herein.

    3. **Governing Law**. This DPA will be governed by and construed in accordance with the laws of the jurisdiction selected in the Agreement, without regard to conflict of law principles, unless required otherwise by Data Protection Laws.

    4. **Notice**. Any notices that are required to be provided in this DPA shall be provided in accordance with any notice provision of the Agreement, unless otherwise specified.

    5. **Authorization**. Customer represents that it is authorized to agree to and enter into this DPA.

ANNEX A TO DPA

DESCRIPTION OF THE PROCESSING

1. **Subject Matter and Details of the Processing**

The Parties acknowledge and agree that (i) the subject matter of the Processing under the Agreement is Company's provision of the Services; (ii) the duration of the Processing is from Company's receipt of Personal Data until deletion of all Personal Data by Company in accordance with the Agreement; (iii) the nature and purpose of the Processing is to provide the Services and as permitted in accordance with the Agreement; (iv) the Data Subjects to whom the Personal Data pertains are Customer's End Users; and (v) the categories of Personal Data can include names, email addresses, phone numbers, physical street addresses, or any other categories of Personal Data that Customer transfers using the Services.

1. **Types of Personal Data**

- Names
- Email addresses
- Phone numbers
- Physical street addresses
- Other types that Customer chooses to transfer using the Services

3. Categories of Data Subjects

- Customer's End Users
- Other categories that Customer chooses to transfer using the Services

4. Categories of Sensitive Data

- None.

5. Obligations and Rights of the Controller

The obligations and rights of Customer are as set out in the Agreement and the DPA.

ANNEX B TO DPA

PROVISIONS APPLICABLE TO PROCESSING OF PERSONAL DATA SUBJECT TO EU DATA PROTECTION LAWS

The provisions of this Annex B will apply to the Processing by Company of Personal Data under the Agreement, but only to the extent that the Processing of Personal Data is subject to EU Data Protection Laws. In the event of any conflict between the provisions of this Annex B and the DPA or the Agreement, the provisions of this Annex B shall control.

1. **Processing of Personal Data.**
    1. **Roles of the Parties.** When Processing Personal Data that is subject to EU Data Protection Law in accordance with Customer's instructions, the Parties acknowledge that Customer is the Controller of the Personal Data and Company is the Processor.
    2. **Legality of Processing Instructions.** Company shall immediately inform Customer in writing, including by electronic mail, if it believes that an instruction of Customer relating to the Processing of Personal Data infringes on EU Data Protection Laws.
2. **Subprocessors**.
    1. **Communication of Changes to the Subprocessor List.** If Company intends to add or replace any Subprocessor in the Subprocessor list in Annex D, as generally authorized in Section 3.1

of the DPA, Company shall inform Customer of the changes and provide Customer the opportunity to object to these changes pursuant to Section 2(b) of this Annex B.

2. **Objection to New Subprocessors**. If Customer has an objection to the addition of a new Subprocessor to the Subprocessor List in accordance with Section 3of the DPA, Customer must notify Company of the objection in writing within ten (10) calendar days of the addition of the new Subprocessor to the Subprocessor List. If Customer does not notify Company in writing of an objection within ten (10) calendar days, Customer waives any objection that it may have had to the new Subprocessor. If Customer submits an objection in accordance with this Section 2, the Parties agree to discuss Customer's concerns in good faith with a view toward achieving a commercially reasonable resolution. If no such resolution can be reached within thirty (30) calendar days, Company may, at its option, either withdraw the objectionable Subprocessor and either perform the Services itself, or appoint a new Subprocessor in accordance with the terms of Section 3of the DPA. The parties agree that by complying with this Section 2, Company fulfills its obligations under Section 9 of the Standard Contractual Clauses.

3. **Subprocessor Contractual Terms.** Company will contractually impose data protection obligations on its Subprocessors that are equivalent to those data protection obligations imposed on Company under the DPA and this Annex B.

4. **Liability for Acts/Omissions of Subprocessors.** Company shall remain liable for the acts and omissions of its Subprocessors to the same extent that Company would be liable if it performed the services of each Subprocessor directly under the terms of this DPA.

3. **Data Subject Requests.** Taking into account the nature of the Processing, Company shall assist Customer by appropriate technical and organizational measures, insofar as it is possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request.

4. **Data Protection Impact Assessment.** To the extent required under applicable EU Data Protection Laws, Company shall (taking into account the nature of the processing and the information available to Company) provide all reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with Supervisory Authorities as required by EU Data Protection Laws. Company shall comply with the foregoing by: (i) complying with Section 5 (Audits) of this Annex B; (ii) providing the information contained in the Agreement, including this DPA; and (iii) if the foregoing subsections (i) and (ii) are insufficient for Customer to comply with such obligations, upon request, providing additional reasonable assistance (at Customer's expense).

5. **Audits.**
    1. **Audits Generally.** Company will make information reasonably necessary to demonstrate compliance with this DPA available to Customer. Customer may audit Company's compliance with its obligations under this DPA up to once per year and on such other occasions as may be required by applicable Data Protection Laws, including where mandated by Customer's Supervisory Authority. Any audit must be conducted during regular

business hours, subject to the agreed final audit plan as set forth in Section 5.3 of this Annex B and subject to Company's safety, security or other relevant policies, and may not unreasonably interfere with Company's business activities.

2. **Third Party Auditors.** If a third party is to conduct an audit under Section 5.1 of this Annex B, Company may object to the auditor if the auditor is, in Company's reasonable opinion, a competitor of Company. Such objection by Company will require Customer to appoint another auditor or conduct the audit itself. Customer will be responsible for all fees charged by any auditor appointed by Customer to execute any audit under this Section 5.

3. **Audit Plan.** Aside from an audit of a Supervisory Authority, to request an audit, Customer must submit a detailed proposed audit plan to Company at least thirty (30) calendar days in advance of the proposed audit date and any third party auditor must sign a customary non-disclosure agreement mutually acceptable to the Parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the scope, duration and start date of the audit. Company will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Company's security, privacy, employment or other relevant policies). Company will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 5.3 shall require Company to disclose any information where such disclosure would result in a breach of any duty of confidentiality.

4. **Third Party Audit Reports.** If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2 or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request and Company has confirmed there are no known material changes in the controls audited, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures.

5. **Subprocessor Information.** Nothing in this Section 5 shall be construed to require Company to furnish more information about its Subprocessors in connection with such audits than such Subprocessors make available to Company without restriction on further disclosure.

6. **Audit Reports.** Customer will promptly notify Company of any non-compliance discovered during the course of an audit and provide Company any audit reports generated in connection with any audit under this Section 5 unless prohibited by applicable Data Protection Laws or otherwise instructed by a Supervisory Authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA. If any audit reveals that Company is not in compliance with the provisions of this DPA and/or applicable EU Data Protection Laws, Company shall take commercially reasonable corrective actions, including temporary workarounds reasonably necessary to comply with the provisions of this DPA and/or applicable EU Data Protection Laws.

6. **Cross-Border Data Transfers.**
    1. **Processing in the United States.** Customer acknowledges that, as of the date of this DPA, Company's processing facilities are located in the United States of America.
    2. **EU Standard Contractual Clauses.** For data transfers to a Third Country, Module Two of the EU Standard Contractual Clauses will apply. The Company shall, and where relevant shall procure that any of its affiliates, sub-processors, or subcontractors shall, comply with the processor's obligations set out in Section II (*Obligations of the Parties*) and with Clause 10(d) of the EU Standard Contractual Clauses and the Customer will comply with the data exporter's obligations in such EU Standard Contractual Clauses, which are hereby incorporated into and form part of this DPA in the following manner:
        1. In Clause 7, the optional docking clause will not apply;
        2. In Clause 9(a), Option 2 will apply, and the time period for notice of Subprocessor changes will be as set forth in Section 3.2 (Subprocessing) of the DPA;
        3. In Clause 11, the optional language will not apply;
        4. In Clause 17, Option 1 will apply, and the EU Standard Contractual Clauses will be governed by Irish law;
        5. In Clause 18(b), disputes will be resolved before the courts of Ireland;
        6. In Annex 1, Part A:
            1. Data Exporter: Customer and authorized affiliates of Customer;
            2. Contact Details: Customer's email address, or the email address(es) for which Customer elects to receive privacy communications.
            3. Data Exporter Role: The Data Exporter's role is defined in Section 2 of this DPA.
            4. Signature & Date: By entering into this DPA, Data Exporter is deemed to have signed the EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the date of this DPA.
            5. Data Importer: Simpler Postage Inc. (d/b/a/ EasyPost)
            6. Contact Details: legal@easypost.com
            7. Data Importer Role: The Data Importer's role is outlined in Section 2 of this DPA.
            8. Signature & Date: By entering into this DPA, Data Importer is deemed to have signed the EU Standard Contractual Clauses

incorporated herein, including their Annexes, as of the date of this DPA.

7. In Annex I, Part B:
    1. The categories of Data Subjects are described in Annex A, Section 3 to this DPA.
    2. The Sensitive Data transferred is described in Annex A, Section 4 to this DPA.
    3. The frequency of the transfer is a continuous basis for the duration of the Agreement.
    4. The nature of the processing is described in Annex A, Section 1 to this DPA.
    5. The purpose of the processing is described in Annex A, Section 1 to this DPA.
    6. The period of the processing is described in Annex A, Section 1 to this DPA.
    7. For transfers to Subprocessors, the subject matter of the processing is as outlined in Annex A, Section 1 to this DPA.
    8. For transfers to Subprocessors, the nature of the processing is as outlined in Annex A, Section 1 to this DPA.
    9. For transfers to Subprocessors, the duration of the processing is as outlined in Annex A, Section 1 to this DPA.
8. For clause 13 and Annex I, Part C, the competent Supervisory Authority is Ireland.
9. Company's SOC 2 Type 2 serves as Annex II to the EU Standard Contractual Clauses.
10. Annex D serves as Annex III to the EU Standard Contractual Clauses.

3. The Customer acknowledge and agree that the Company may appoint an affiliate or third-party subcontractor to Process the Company's Personal Data in a Third Country, in which case, the Company shall execute the Processor to Processor Clauses with any relevant subcontractor (including affiliates) it appoints on behalf of the Customer.
4. **U.K. Standard Contractual Clauses.** For data transfers from the United Kingdom to a Third Country, the U.K. Standard Contractual Clauses will apply. The Company shall comply with the processor's obligations in the U.K. Standard Contractual Clauses and the Customer will

comply with the data exporter's obligations in such U.K. Standard Contractual Clauses, which are hereby incorporated into and form part of this DPA in the following manner:

1. The illustrative indemnification clause will not apply;
2. the Company (as importer) may terminate the U.K. Standard Contractual Clauses pursuant to Section 19;
3. Annex A and the relevant provisions set out in 6(b) above serve as Appendix 1 to the U.K. Standard Contractual Clauses;
4. Company's SOC 2 Type 2 serves as Appendix 2 to the U.K. Standard Contractual Clauses; and
5. Annex D serves as Appendix 3 to the U.K Standard Contractual Clauses.

5. **Conflicts.** To the extent there is any conflict between the EU Standard Contractual Clauses or the U.K. Standard Contractual Clauses and any other terms in this DPA, including Section 8.1 (Jurisdiction Specific Terms), the provisions of the EU Standard Contractual Clauses will prevail, but only to the extent that the EU Standard Contractual Clauses and/or the U.K. Standard Contractual Clauses apply.
6. **Amendments to EU Standard Contractual Clauses or U.K. Standard Contractual Clauses**. If the European Commission, the United Kingdom Information Commissioner's Office or a Supervisory Authority amends the EU Standard Contractual Clauses or the U.K. Standard Contractual Clauses, the parties shall promptly discuss the proposed amendments and negotiate in good faith with a view toward agreeing and implementing those amendments as soon as is reasonably practicable.

ANNEX C TO DPA

PROVISIONS APPLICABLE TO PROCESSING OF PERSONAL DATA

SUBJECT TO US DATA PROTECTION LAWS

The provisions of this Annex C will apply to the Processing by Company of Personal Data under the Agreement, but only to the extent that Customer and the Personal Data are subject to US Data Protection Laws. In the event of any conflict between the provisions of this Annex C and the DPA or the Agreement, the provisions of this Annex C shall control.

1. **Definitions.** As used in this Annex C, the terms "**Business Purpose**", "**Commercial Purpose**", "**Deidentified**", "**Sell**", "**Sale**", "**Share**" and "**Sharing**" shall have the same meaning as in US Data Protection Laws, as applicable.
2. **Roles of the Parties.** The Parties acknowledge and agree that, with regard to the Processing of Personal Data on behalf of Customer, Company is a Processor and/or Service Provider and receives Personal

Data on Customer's behalf to provide the Services or as otherwise permitted by US Data Protection Laws. Further information regarding the nature and purpose of Processing, the categories of Personal Data, categories of Data Subjects and duration of Processing are set forth in Annex A. To the extent Company receives Personal Data from Customer that has been Deidentified, Company will maintain and use the data only in Deidentified fashion.

3. **No Sale or Sharing of Personal Data to Company.** Customer and Company hereby acknowledge and agree that in no event shall the transfer of Personal Data from Customer to Company pursuant to the Agreement constitute the Sale or Sharing of Personal Data to Company, and that nothing in the Agreement shall be construed as providing for the Sale or Sharing of Personal Data.

4. **Company Obligations.** With regard to the Processing of Personal Data performed solely on behalf of Customer, Company will, to the extent required by US Data Protection Laws:
    1. not retain, use or disclose the Personal Data outside of the direct business relationship with Customer or for any purposes other than to provide the Services, including retaining, using or disclosing Personal Data for a Commercial Purpose other than performing the Business Purposes specified in the Agreement, unless otherwise permitted by US Data Protection Laws.
    2. not Sell or Share such Personal Data;
    3. in connection with Processing the Personal Data, comply with provisions of US Data Protection Laws applicable to Service Providers or Processors, including providing the same level of privacy protection required of Businesses or Controllers by US Data Protection Laws, and notify Customer in writing (including by email) if Company determines that it can no longer meet these obligations. Customer may, upon receiving such a notice, take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data by Company;
    4. not combine Personal Data that Company receives from, or on behalf of, Customer with Personal Data that it receives from another source or collects from its own interaction with the Data Subject, except to perform the Services, with consent or direction, or as otherwise permitted by US Data Protection Laws;
    5. only engage Subprocessors to process Personal Data on Company's behalf pursuant to a written contract that requires comparable protections to this DPA and, if applicable under US Data Protection Laws, provide Customer with written notice and a reasonable opportunity to object to the use of such Subprocessor. A current list of Subprocessors may be found in Annex D;
    6. ensure that Company's personnel who process the Personal Data are subject to confidentiality obligations with respect to such data;
    7. take reasonable and appropriate steps, upon reasonable written notice from Customer and subject to any confidentiality obligations set out in the Agreement, to assist Customer with

confirming Company's use of Personal Data is consistent with Customer's obligations under US Data Protection Laws;

8. allow for reasonable audits by Customer or Customer's designated auditor, upon thirty (30) days written notice, and at Customer's expense, of Company's compliance with applicable US Data Protection Laws no more than once every twelve (12) months, provided that such audits occur during regular business hours under a duty of confidentiality and do not unreasonably impact in an adverse manner Company's regular operations. Alternatively, Company may arrange for a qualified and independent auditor to conduct an annual assessment of Company's policies and technical and organizational measures in support of its obligations under applicable US Data Protection Laws using an appropriate and accepted control standard or framework and assessment procedure for such assessments. Company shall provide a report to Customer upon request; and
9. upon termination of the Agreement at Customer's written election, return or delete the Personal Data, unless retention of the Personal Data is required by law.

5. **Customer's Obligations.** Customer represents and warrants that it will:
6. not share with Company any Personal Data of any Data Subject who has exercised a right to opt-out that Customer has committed to honoring;
7. not share with Company Sensitive Data of any Data Subject who has not consented to the Processing of their Sensitive Data; and
8. inform Company of any Data Subject Request an individual makes to Customer pursuant to US Data Protection Laws that they must comply with and provide the information necessary for Company to comply with the requests.

ANNEX D TO DPA

LIST OF SUBPROCESSORS

Alphabet, Inc.	Communications and data storage	USA
Amazon Web Services	Data center hosting	USA
Dash Networks, Inc. d/b/a Enzu	Data center hosting	USA
Digital Realty Trust	Data center hosting	USA

DigitalOcean, Inc.	Data storage	USA
Functional Software, Inc. / Sentry.io	Data storage	USA
Hubspot, Inc.	Partner relationship management	USA
IBM's Softlayer	Data center hosting	USA
Microsoft Corporation	Cloud Hosting, Storage, and IT Services	USA
Polytomic, Inc.	Data storage	USA
Salesforce Inc	Partner relationship management	USA
Twilio, Inc. / Sendgrid	Communications and data storage	USA