LEGAL

Data Processing Addendum

In this document

This Data Processing Addendum ("**DPA**") is incorporated into, and is subject to the terms and conditions of, the Agreement between The Rocket Science Group LLC d/b/a Mailchimp (together with its Affiliates, "**Mailchimp**") and the customer entity that is a party to the Agreement ("**Customer**" or "**you**").

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. For the avoidance of doubt, all references to the "Agreement" shall include this DPA (including the SCCs (where applicable), as defined herein).

1. Definitions

"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

"**Agreement**" means Mailchimp's **Standard Terms of Use**, or other written or electronic agreement, which govern the provision of the Service to Customer, as such terms or agreement may be updated from time to time.

"**Control**" means an ownership, voting or similar interest representing fifty percent

(50%) or more of the total interests then outstanding of the entity in question. The term "**Controlled**" shall be construed accordingly.

"**Customer Data**" means any personal data that Mailchimp processes on behalf of Customer via the Service, as more particularly described in this DPA.

"**Data Protection Laws**" means all data protection laws and regulations applicable to a party's processing of Customer Data under the Agreement, including, where applicable, EU Data Protection Law and Non-EU Data Protection Laws.

"**EU Data Protection Law**" 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); and (iii) 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).

"**Europe**" means, for the purposes of this DPA, the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

"**Non-EU Data Protection Laws**" means the California Consumer Privacy Act ("CCPA"); the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); and the Brazilian General Data Protection Law ("LGPD"), Federal Law no. 13,709/2018.

"**Privacy Shield**" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce.

"**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles).

"**SCCs**" means the standard contractual clauses for processors as approved by the European Commission or Swiss Federal Data Protection Authority (as applicable).

"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Customer Data on systems managed or otherwise controlled by Mailchimp.

"**Sensitive Data**" means (a) social security 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, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords; or (f) other information that falls within the definition of "special categories of data" under applicable Data Protection Laws.

"**Service Data**" means any data relating to the Customer's use, support and/or operation of the Service, including information relating to volumes, activity logs, frequencies, bounce rates or other information regarding emails and other communications Customer generates and sends using the Service.

"**Sub-processor**" means any processor engaged by Mailchimp or its Affiliates to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA. Sub-processors may include third parties or Affiliates of Mailchimp but shall exclude Mailchimp employees or consultants.

The terms "**personal data**", "**controller**", "**data subject**", "**processor**" and "**processing**" shall have the meaning given to them under Data Protection Laws or if not defined thereunder, the GDPR, and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly.

2. Roles and Responsibilities

2.1 **Parties' roles**. If EU Data Protection Law or the LGPD applies to either party's processing of Customer Data, the parties acknowledge and agree that with regard to

the processing of Customer Data, Customer is the controller and Mailchimp is a processor acting on behalf of Customer, as further described in Annex A (Details of Data Processing) of this DPA.

2.2 **Purpose limitation**. Mailchimp shall process Customer Data only in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, or as otherwise agreed in writing ("Permitted Purposes"). The parties agree that the Agreement sets out Customer's complete and final instructions to Mailchimp in relation to the processing of Customer Data, and processing outside the scope of these instructions (if any) shall require prior written agreement between the parties.

2.3 **Prohibited data**. Customer will not provide (or cause to be provided) any Sensitive Data to Mailchimp for processing under the Agreement, and Mailchimp will have no liability whatsoever for Sensitive Data, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, this DPA will not apply to Sensitive Data.

2.4 **Customer compliance**. 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 Customer Data and any processing instructions it issues to Mailchimp; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for Mailchimp to process Customer Data for the purposes described in the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which Customer acquired Customer 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 emails or other content created, sent or managed through the Service, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices.

2.5 **Lawfulness of Customer's instructions**. Customer will ensure that Mailchimp's processing of the Customer Data in accordance with Customer's instructions will not cause Mailchimp to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws. Mailchimp shall promptly notify Customer in writing,

unless prohibited from doing so under EU Data Protection Laws, if it becomes aware or believes that any data processing instruction from Customer violates the GDPR or any UK implementation of the GDPR.

3. Sub-processing

3.1 **Authorized Sub-processors**. Customer agrees that Mailchimp may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by Mailchimp and authorized by Customer are available **here**. Mailchimp shall notify Customer if it adds or removes Sub-processors at least 10 days prior to any such changes if Customer opts in to receive such notifications by clicking **here**.

3.2 **Sub-processor obligations**. Mailchimp shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Data as those in this DPA, to the extent applicable to the nature of the service provided by such Sub-processor; and (ii) remain responsible for such Sub-processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-processor that cause Mailchimp to breach any of its obligations under this DPA.

4. Security

4.1 **Security Measures**. Mailchimp shall implement and maintain appropriate technical and organizational security measures that are designed to protect Customer Data from Security Incidents and designed to preserve the security and confidentiality of Customer Data in accordance with Mailchimp's security standards described in **Annex B** ("**Security Measures**").

4.2 **Confidentiality of processing**. Mailchimp shall ensure that any person who is authorized by Mailchimp to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.3 **Updates to Security Measures**. Customer is responsible for reviewing the information made available by Mailchimp relating to data security and making an independent determination as to whether the Service meets Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Mailchimp 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 Service provided to Customer.

4.4 **Security Incident response**. Upon becoming aware of a Security Incident, Mailchimp shall: (i) notify Customer without undue delay, and where feasible, in any event no later than 48 hours from becoming aware of the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) promptly take reasonable steps to contain and investigate any Security Incident. Mailchimp's notification of or response to a Security Incident under this Section 4.4 shall not be construed as an acknowledgment by Mailchimp of any fault or liability with respect to the Security Incident.

4.5 **Customer responsibilities**. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Service, and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Service.

5. Security Reports and Audits

5.1 **Audit rights**. Mailchimp shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections by Customer in order to assess compliance with this DPA. Customer acknowledges and agrees that it shall exercise its audit rights under this DPA (including this Section 5.1 and where applicable, the SCCs) and any audit rights granted by Data Protection Laws, by instructing Mailchimp to comply with the audit measures described in Sections 5.2 and 5.3 below.

5.2 **Security reports.** Customer acknowledges that Mailchimp is regularly audited against SSAE 16 and PCI standards by independent third party auditors and internal auditors respectively. Upon written request, Mailchimp shall supply (on a confidential basis) a summary copy of its most current audit report(s) ("**Report**") to Customer, so that Customer can verify Mailchimp's compliance with the audit standards against which it has been assessed and this DPA.

5.3 **Security due diligence**. In addition to the Report, Mailchimp shall respond to all reasonable requests for information made by Customer to confirm Mailchimp's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon Customer's written request to **privacy@mailchimp.com**, provided that Customer shall not exercise this right more than once per calendar year.

6. International Transfers

6.1 **Data center locations**. Customer acknowledges that Mailchimp may transfer and process Customer Data to and in the United States and anywhere else in the world where Mailchimp, its Affiliates or its Sub-processors maintain data processing operations. Mailchimp shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws.

6.2 **European Data transfers**. To the extent that Mailchimp is a recipient of Customer Data protected by EU Data Protection Laws ("EU Data"), the parties agree that Mailchimp makes available the mechanisms listed below:

- (a) **Privacy Shield**: For as long as Mailchimp is self-certified to the Privacy Shield: (i) the parties acknowledge and agree that Mailchimp will be deemed to provide adequate protection (within the meaning of applicable EU Data Protection Laws) for EU Data by virtue of having self-certified its compliance with Privacy Shield; (ii) Mailchimp agrees to process EU Data in compliance with the Privacy Shield Principles; and (iii) if Mailchimp is unable to comply with this requirement, Mailchimp shall inform Customer.
- (b) **SCCs**: Mailchimp agrees to abide by and process EU Data in compliance with the SCCs, which are incorporated in full by reference and form an

integral part of this DPA. For the purposes of the SCCs: (i) Mailchimp agrees that it is the "data importer" and Customer is the "data exporter" under the SCCs (notwithstanding that Customer may itself be an entity located outside the EU); (ii) Annexes A and B of this DPA shall replace Appendixes 1 and 2 of the SCCs, respectively; and (iii) Annex C shall form Appendix 3 of the SCCs. The parties further agree that the SCCs will apply to Customer Data that is transferred via the Service from Europe to outside Europe, either directly or via onward transfer, to any country or recipient: (a) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Law); and (b) not covered by Mailchimp's Privacy Shield certification.

7. Return or Deletion of Data

7.1 **Deletion on termination.** Upon termination or expiration of the Agreement, Mailchimp shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control, except that this requirement shall not apply to the extent Mailchimp is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Mailchimp shall securely isolate, protect from any further processing and eventually delete in accordance with Mailchimp's deletion policies, except to the extent required by applicable law.

8. Data Subject Rights and Cooperation

8.1 **Data subject requests.** As part of the Service, Mailchimp provides Customer with a number of self-service features, that Customer may use to retrieve, correct, delete or restrict the use of Customer Data, which Customer may use to assist it in connection with its obligations under the Data Protection Laws with respect to responding to requests from data subjects via Customer's account at no additional cost. In addition, Mailchimp shall, taking into account the nature of the processing, provide reasonable additional assistance to Customer to the extent possible to enable Customer to comply with its data protection obligations with respect to data subject rights under Data Protection Laws. In the event that any such request is made

to Mailchimp directly, Mailchimp shall not respond to such communication directly except as appropriate (for example, to direct the data subject to contact Customer) or legally required, without Customer's prior authorization. If Mailchimp is required to respond to such a request, Mailchimp shall promptly notify Customer and provide Customer with a copy of the request unless Mailchimp is legally prohibited from doing so. For the avoidance of doubt, nothing in the Agreement (including this DPA) shall restrict or prevent Mailchimp from responding to any data subject or data protection authority requests in relation to personal data for which Mailchimp is a controller.

8.2 **Subpoenas and court orders**. If a law enforcement agency sends Mailchimp a demand for Customer Data (for example, through a subpoena or court order), Mailchimp shall attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Mailchimp may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Mailchimp shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy, unless Mailchimp is legally prohibited from doing so.

8.3 **Data protection impact assessment**. To the extent required under applicable Data Protection Laws, Mailchimp shall (taking into account the nature of the processing and the information available to Mailchimp) provide all reasonably requested information regarding the Service to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws. Mailchimp shall comply with the foregoing by: (i) complying with Section 5 (Security Reports and Audits); (ii) providing the information contained in the Agreement, including this DPA; and (iii) if the foregoing sub-sections (i) and (ii) are insufficient for Customer to comply with such obligations, upon request, providing additional reasonable assistance (at Customer's expense).

9. Jurisdiction-Specific Terms

To the extent Mailchimp processes Customer Data originating from and protected by Data Protection Laws in one of the jurisdictions listed in Annex D, then the terms specified in Annex D with respect to the applicable jurisdiction(s) ("Jurisdiction-

Specific Terms") apply in addition to the terms of this DPA. In the event of any conflict or ambiguity between the Jurisdiction-Specific Terms and any other terms of this DPA, the applicable Jurisdiction-Specific Terms will take precedence, but only to the extent of the Jurisdiction-Specific Terms' applicability to Mailchimp.

10. Limitation of Liability

10.1 Each party's and all of its 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.

10.2 Any claims made against Mailchimp 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.

10.3 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

11. Relationship with the Agreement

11.1 This DPA shall remain in effect for as long as Mailchimp carries out Customer Data processing operations on behalf of Customer or until termination of the Agreement (and all Customer Data has been returned or deleted in accordance with Section 7.1 above).

11.2 The parties agree that this DPA shall replace any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Service.

11.3 In the event of any conflict or inconsistency between this DPA and the Mailchimp Standard Terms of Use, the provisions of the following documents (in order of precedence) shall prevail: (a) SCCs; then (b) this DPA; and then (c) the Mailchimp Standard Terms of Use.

11.4 Except for any changes made by this DPA, the Agreement remains unchanged and in full force and effect.

11.5 Notwithstanding anything to the contrary in the Agreement (including this DPA), Mailchimp shall have a right to collect, use and disclose Service Data for its legitimate business purposes, such as: (i) for accounting, tax, billing, audit, and compliance purposes; (ii) to provide, develop, optimize and maintain the Service; (iii) to investigate fraud, spam, wrongful or unlawful use of the Service; and/or (iv) as required by applicable law.

To the extent any such Service Data is considered personal data under Data Protection Laws, Mailchimp shall be responsible for and shall process such data in accordance with the **Mailchimp Privacy Policy** and Data Protection Laws. For the avoidance of doubt, this DPA shall not apply to Service Data.

11.6 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

11.7 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

Annex A – Details of Data Processing

(a) **Subject matter**: The subject matter of the data processing under this DPA is the Customer Data.

(b) **Duration of processing**: Mailchimp will process Customer Data as outlined in Section 7 (Return or Deletion of Data) of this DPA.

(c) **Purpose of processing**: Mailchimp shall only process Customer Data for the Permitted Purposes, which shall include: (i) processing as necessary to provide the Service in accordance with the Agreement; (ii) processing initiated by Customer in its use of the Service; and (iii) processing to comply with any other reasonable instructions provided by Customer (e.g., via email or support tickets) that are

consistent with the terms of the Agreement.

(d) **Nature of the processing**: Mailchimp provides an email service, automation and marketing platform and other related services, as more particularly described in the Agreement.

(e) **Categories of data subjects**: (i) Members; and (ii) Contacts, each as defined in the Mailchimp Privacy Policy.

(f) **Types of Customer Data**: Customer may upload, submit or otherwise provide certain personal data to the Service, the extent of which is typically determined and controlled by Customer in its sole discretion, and may include the following types of personal data:

- **Members**: Identification and contact data (name, address, title, contact details, username); financial information (credit card details, account details, payment information); employment details (employer, job title, geographic location, area of responsibility);
- **Contacts**: Identification and contact data (name, date of birth, gender, general, occupation or other demographic information, address, title, contact details, including email address); personal interests or preferences (including purchase history, marketing preferences and publicly available social media profile information); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data); financial information (credit card details, account details, payment information).

(g) **Sensitive Data**: Mailchimp does not want to, nor does it intentionally, collect or process any Sensitive Data in connection with the provision of the Service.

(h) **Processing Operations**: Customer Data will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities:

- Storage and other processing necessary to provide, maintain and improve the Service provided to Customer pursuant to the Agreement; and/or
- Disclosures in accordance with the Agreement and/or as compelled by applicable law.

Annex B – Security Measures

The Security Measures applicable to the Service are described **here** (as updated from time to time in accordance with Section 4.3 of this DPA).

Annex C

All defined terms used in this Annex C shall have the meaning given to them in the SCCs unless otherwise defined in this Annex.

Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

For the purposes of this Appendix, "DPA" means the Data Processing Addendum in place between data importer and data exporter and to which these Clauses are incorporated and "Agreement" shall have the meaning given to it in the DPA.

Clause 5(a): Suspension of data transfers and termination

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled

to suspend the transfer of data and/or terminate the Clauses.

3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").
4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 5 (Security Reports and Audits) of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.
2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.
3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not to limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability with

respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward subprocessing by the data importer.
2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in Section 3 (Sub-processing) of the DPA.

Annex D - Jurisdiction-Specific Terms

Europe:

1. Objection to Sub-processors. Customer may object in writing to Mailchimp's appointment of a new Sub-processor within five (5) calendar days of receiving notice in accordance with Section 3.1 of DPA, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Mailchimp will, at its sole discretion, either not appoint such Sub-processor, or permit Customer to suspend or terminate the affected Service in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

California:

1. The definitions of: "controller" includes "Business"; "processor" includes "Service Provider"; "data subject" includes "Consumer"; "personal data" includes "Personal Information"; in each case as defined under CCPA.

2. For this “California” section of Annex D only, “Mailchimp Services” means the suite of marketing tools and insights available for Mailchimp Customers to use, including without limitation, email campaign management, advertisements, and direct mailings and other related digital communications, analytics and tools made available through the Mailchimp online marketing platform, as may be further described in the App and/or on the Mailchimp Site.
3. For this “California” section of Annex D only, “Permitted Purposes” shall include processing Customer Data only for the purposes described in this DPA and in accordance with Customer’s documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, as otherwise agreed in writing, or as otherwise may be permitted for “service providers” under the CCPA.
4. Mailchimp’s obligations regarding data subject requests, as described in Section 8 (Data Subject Rights and Cooperation) of this DPA, apply to Consumer’s rights under the CCPA.
5. Notwithstanding any use restriction contained elsewhere in this DPA, Mailchimp shall process Customer Data only to perform the Mailchimp Services, for the Permitted Purposes and/or in accordance with Customer’s documented lawful instructions, except where otherwise required by applicable law.
6. Mailchimp may de-identify or aggregate Customer Data as part of performing the Service specified in this DPA and the Agreement.
7. Where Sub-processors process the personal data of Customer contacts, Mailchimp takes steps to ensure that such Sub-processors are Service Providers under the CCPA with whom Mailchimp has entered into a written contract that includes terms substantially similar to this DPA or are otherwise exempt from the CCPA’s definition of “sale”. Mailchimp conducts appropriate due diligence on its Sub-processors.

Canada:

1. Mailchimp takes steps to ensure that Mailchimp's Sub-processors, as described in Section 3 (Sub-processing) of the DPA, are third parties under PIPEDA, with whom Mailchimp has entered into a written contract that includes terms substantially similar to this DPA. Mailchimp conducts appropriate due diligence on its Sub-processors.
2. Mailchimp will implement technical and organizational measures as set forth in Section 4 (Security) of the DPA.

Effective January 1, 2020