LEGAL

# Data Processing Addendum

Download

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 as a Member ("Customer").

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, European Data Protection Laws and Non-European Data Protection Laws.

**"European 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) the GDPR as it forms part of UK law by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (together, "UK Data Protection Laws"); and (v) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance ("Swiss DPA").

**"Europe"** means, for the purposes of this DPA, the European Economic Area and its member states ("EEA"), Switzerland and the United Kingdom ("UK").

**"Non-European Data Protection Laws"** means the California Consumer Privacy Act ("CCPA"); the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); the Brazilian General Data Protection Law ("LGPD"), Federal Law no. 13,709/2018; and the Privacy Act 1988 (Cth) of Australia, as amended ("Australian Privacy Law").

**"SCCs"** means either (i) the standard contractual clauses between controllers and processors adopted by the European Commission in its Implementing Decision 2010/87/EU of 5 February 2010, and currently located **here** (the "2010 Controller-to-Processor Clauses"); (ii) the standard contractual clauses between controllers and processors adopted by the European Commission in its Implementing Decision (EU) 2021/91 of 4 June 2021, and currently located **here** (the "2021 Controller-to-Processor Clauses"); or (iii) the standard contractual clauses between processors adopted by the European Commission in its Implementing Decision (EU) 2021/91 of 4 June 2021, and currently located **here** (the "2021 Processor-to-Processor Clauses"); as applicable in accordance with Section 6.3.

**"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, tax file number, passport numbe 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" under applicable Data Protection Laws.

**"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, contractors, or consultants.

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

## 2. Roles and Responsibilities

2.1 **Parties' roles.** If European Data Protection Laws 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, Mailchimp is a processor acting on behalf of Customer (whether itself a controller or a processor). For the avoidance of doubt, this DPA shall not apply to instances where Mailchimp is the controller (as defined by European Data Protection Laws) unless otherwise described in Annex C (Jurisdiction-Specific Terms) of this DPA.

2.2 **Purpose limitation.** Mailchimp shall process Customer Data, as further described in Annex A (Details of Data Processing) of this DPA, 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, including this DPA, along with the Customer's configuration of or use of any settings, features, or options in the Service (as the Customer may be able to modify from time to time) constitute the Customer's complete and final instructions to Mailchimp in relation to the processing of Customer Data (including for the purposes of the SCCs), 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 Campaigns (as defined in the Agreement) 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 European Data Protection Laws, if it becomes aware or believes that any data processing instruction from Customer violates European Data Protection Laws. Where Customer acts as a processor on behalf of a third-party controller (or other intermediary to the ultimate controller), Customer warrants that its processing instructions as set out in the Agreement and this DPA, including its authorizations to Mailchimp for the appointment of Sub-processors in accordance with this DPA, have been authorized by the relevant controller. Customer shall serve as the sole point of contact for Mailchimp and Mailchimp need not interact directly with (including to provide notifications to or seek authorization from) any third-party controller other than through regular provision of the Service to the extent required under the Agreement. Customer shall be responsible for forwarding any notifications received under this DPA to the relevant controller, where appropriate.

# 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 day prior to any such changes if Customer opts in to receive such notifications by clicki **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. Customer acknowledges and agrees that, where applicable, Mailchimp fulfills its obligations under Clause 9 of the 2021 Controller-to-Processor Clauses and 2021 Processor-to-Processor Clauses (as applicable) by complying with this Section 3 and that Mailchimp may be prevented from disclosing Sub-processor agreements to Customer due to confidentiality restrictions but Mailchimp shall, upon request, use reasonable efforts to provide Customer with all relevant information it reasonably can in connection with Subprocessor agreements.

# 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") of this DPA.

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 conta

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.** Subject to Section 6.2, 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 and this DPA.

6.2 **Australian data.** To the extent that Mailchimp is a recipient of Customer Data protected by the Australian Privacy Law, the parties acknowledge and agree that Mailchimp may transfer such Customer Data outside of Australia as permitted by the terms agreed upon by the parties and subject to Mailchimp complying with this DPA and the Australian Privacy Law.

6.3 **European Data transfers.** To the extent that Mailchimp is a recipient of Customer Data protected by European Data Protection Laws ("European Data") in a country outside of Europe that is not recognized as providing an adequate level of protection for personal data (as described in applicable European Data Protection Laws), the parties agree to abide by and process European Data in compliance with the SCCs, which shall be incorporated into and form an integral part of this DPA as follows: (a) if Customer started using the Service before 27 September 2021, the 2010 Controller-to-Processor Clauses shall apply (regardless of whether Customer is a controller or a processor) until December 27, 2022, and thereafter the 2021 Controller-to-Processor Clauses and/or the 2021 Processor-to-Processor Clauses shall automatically apply (according to whether Customer is a controller and/or a processor) thereafter; (b) if Customer started using the Service on or after 27 September 2021, the 2021 Controller-to-Processor Clauses and/or the 2021 Processor-to-Processor Clauses shall apply (according to whether Customer is a controller and/or a processor) immediately.

6.4 **Compliance with the SCCs.** The parties agree that if Mailchimp cannot ensure compliance with the SCCs, it shall promptly inform Customer of its inability to comply. If Customer intends to suspend the transfer of European Data and/or terminate the affected parts of the Service, it shall first provide notice to Mailchimp and provide Mailchimp with a reasonable period of time to cure such non-compliance, during which time Mailchimp and Customer shall reasonably cooperate to agree what additional safeguards or measures, if any, may be reasonably required. Customer shall only be entitled to suspend the transfer of data and/or terminate the affected parts of the Service for non-compliance with the SCCs if Mailchimp has not or cannot cure the non-compliance within a reasonable period.

6.5 **Alternative transfer mechanism.** To extent that and for so long as the SCCs as implemented in accordance with Section 6.3 cannot be relied on to lawfully transfer personal data in compliance with UK Data Protection Laws, the standard data protection clauses for processors adopted pursuant to or permitted under Article 46 of the UK GDPR ("UK SCCs") shall be incorporated by reference and deemed completed with relevant information set out in the Annexes of this DPA. Additionally, to the extent

Mailchimp adopts an alternative lawful data transfer mechanism for the transfer of European Data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable European Data Protection Laws and extends to the countries to which European Data is transferred). In addition, if and to the extent that a court of competent jurisdiction or supervisory authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer European Data (within the meaning of applicable European Data Protection Laws), Mailchimp may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of European Data.

## 7. Return or Deletion of Data

Deletion or return 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. The parties agree that the certification of deletion of Customer Data described in Clause 8.5 and 16(d) of the 2021 Controller-to-Processor Clauses and 2021 Processor-to-Processor Clauses (as applicable) shall be provided by Mailchimp to Customer only upon Customer's written request.

## 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 (or its third-party controller's) 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, considering the nature of the processing, provide reasonable additional assistance to Customer to the extent possible to enable Customer (or its third-party controller) 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, where the

Customer is identified or identifiable from the request, 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 **Data protection impact assessment.** To the extent required under applicable Data Protection Laws, Mailchimp shall (considering 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 C, then the terms specified in Annex C 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 Standard Terms of Use, the provisions of the following documents (in order of precedence) shall prevail: (i) SCCs; then (ii) this DPA; and then (iii) the 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 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

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

# Annex A – Details of Data Processing

(a) **Categories of data subjects**:

The categories of data subjects whose personal data is processed include (i) Members (i.e., individual end users with access to a Mailchimp account) and (ii) Contacts (i.e., Member's subscribers and other individuals about whom a Member has given us information or has otherwise interacted with a Member via the Service).

(b) **Categories of personal 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 i 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).

(c) **Sensitive data processed (if applicable)**:

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

(d) **Frequency of processing**:

Continuous and as determined by Customer.

(e) **Subject matter and nature of the processing**:

Mailchimp provides an email service, automation and marketing platform and other related services, as more particularly described in the Agreement. The subject matter of the data processing under this DPA is the Customer Data. 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.

(f) **Purpose of the 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 Agreeme

(g) **Duration of processing and period for which personal data will be retained:**

Mailchimp will process Customer Data as outlined in Section 7 (Return or Deletion of Data) of this DPA.

# 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 - 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 the 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).
2. Government data access requests. As a matter of general practice, Mailchimp does not voluntarily provide government agencies or authorities (including law enforcement) with access to or information about Mailchimp accounts (including Customer Data). If Mailchimp receives a compulsory request (whether through a subpoena, court order, search warrant, or other valid legal process) from any government agency or authority (including law enforcement) for access to or information about a Mailchimp account (including Customer Data) belonging to a Customer whose primary contact information indicates the Customer is located in Europe, Mailchimp shall: (i) review the legality of the request; (ii) inform the government agency that Mailchimp is a processor of the data; (iii) attempt to redirect the agency to request the data directly from Customer; (iv) notify Customer via email sent to Customer's primary contact email address of the request to allow Customer to seek a protective order or other appropriate remedy; and (v) provide the minimum amount of informat permissible when responding to the agency or authority based on a reasonab

interpretation of the request. As part of this effort, Mailchimp may provide Customer's primary and billing contact information to the agency. Mailchimp shall not be required to comply with this paragraph 2 if it is legally prohibited from doing so, or it has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual, public safety, or Mailchimp's property, the Mailchimp Site, or Service, but where Mailchimp is legally prohibited from notifying Customer of requests it shall use its best efforts to obtain a waiver of the prohibition.

California:

1. Except as described otherwise, 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 the CCPA.
2. For this "California" section of Annex C 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, including, without limitation, in the Agreement, or as otherwise may be permitted for "service providers" under the CCPA.
3. Mailchimp's obligations regarding data subject requests, as described in Section 8 (Data Subject Rights and Cooperation) of this DPA, extend to rights requests under the CCPA.
4. Notwithstanding any use restriction contained elsewhere in this DPA, Mailchimp shall process Customer Data to perform the Service, for the Permitted Purposes and/or in accordance with Customer's documented lawful instructions, or as otherwise permitted or required by applicable law.
5. Notwithstanding any use restriction contained elsewhere in this Annex C, Mailchimp may de-identify or aggregate Customer Data as part of performing the Service specified in this DPA and the Agreement.
6. Where Sub-processors process the Personal Information 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 "California" section of Annex C 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 10, 2022*