LEGAL

Data Processing Addendum

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"); 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").

"**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, 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" 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 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. For the avoidance of doubt, this DPA shall not apply to instances where Mailchimp is the controller (as defined by EU Data Protection Law) unless otherwise described in Annex D hereto.

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 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 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**. 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 EU Data Protection Laws ("EU 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 EU Data Protection Law), the parties agree to the following:

- (a) **SCCs**: Mailchimp agrees to abide by and process EU Data in compliance with the SCCs in the form set out in Annex C. For the purposes of the descriptions in the SCCs, Mailchimp agrees that it is the "data importer" and Customer is the

"data exporter" (notwithstanding that Customer may itself be an entity located outside Europe).

- (b) **Privacy Shield**: Although Mailchimp does not rely on the EU-US Privacy Shield as a legal basis for transfers of Customer Data in light of the judgement of the Court of Justice of the EU in Case C-311/18, for as long as Mailchimp is self-certified to the Privacy Shield: (i) Mailchimp agrees to process EU Data in compliance with the Privacy Shield Principles and (ii) if Mailchimp is unable to comply with this requirement, Mailchimp shall inform Customer.

6.4 **Alternative transfer mechanism**. To the extent Mailchimp adopts an alternative data export mechanism (including any new version of or successor to the SCCs or Privacy Shield) for the transfer of EU 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 EU Data Protection Law and extends to the countries to which EU 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 EU Data (within the meaning of applicable EU Data Protection Law), Mailchimp may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of EU 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.

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 **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: (i) SCCs; then (ii) this DPA; and then (iii) 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 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) **Controller (data exporter)**: Customer, being a Mailchimp Member (as defined in the Mailchimp **Privacy Policy**) that has engaged Mailchimp to provide the Service under the Agreement.

(b) **Processor (data importer)**: Mailchimp, a Georgia limited liability company, whose legal name is The Rocket Science Group LLC d/b/a Mailchimp.

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

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

(e) **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.

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

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

(h) **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).

(i) **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.

(j) **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 - Standard Contractual Clauses

Standard Contractual Clauses

2010 Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to processor transfers)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Mailchimp a Georgia limited liability company whose legal name is The Rocket Science Group LLC d/b/a Mailchimp (hereinafter the "**data importer**") and Customer (hereinafter the "**data exporter**") each a "party"; together "the parties", HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex 1.

Clause 1

Definitions

For the purposes of the Clauses:

- **'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'** and **'supervisory authority'** shall have the same

meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

- **'the data exporter'** means the controller who transfers the personal data;
- **'the data importer'** means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- **'the subprocessor'** means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- **'the Data Protection Law'** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- **'technical and organisational security measures'** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law

unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the Data Protection Law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the Data Protection Law and the Clauses;
- that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- that after assessment of the requirements of the Data Protection Law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- that it will ensure compliance with the security measures; that, if the transfer involves special categories of data, the data subject has been informed or will

be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

- to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, 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 contract;
- that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- that it will promptly notify the data exporter about:
    - any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

    - any accidental or unauthorised access, and
    - any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely

on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
    - to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
    - to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the Data Protection Law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the Data Protection Law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In

such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member

State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Details of the transfer:

Please see the details set forth in Annex A to the Data Processing Addendum ("DPA") to which these Clauses are appended.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please see Annex B – Security Measures

APPENDIX 3 TO STANDARD CONTRACTUAL CLAUSES

The parties acknowledge that Clause 10 of the Clauses permits them to include additional business-related terms provided they do not contradict with the Clauses.

Accordingly, 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.

Clauses 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's Confidential Information (as that term is defined in the Agreement) and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to the Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

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

1. The parties acknowledge that for the purposes of Clause 5(a), data importer may process the personal data only on behalf of the data exporter and in compliance with its documented instructions as set out in the DPA and that pursuant to the DPA, these instructions shall be the data exporter’s complete and final instructions.
2. The parties acknowledge that if data importer cannot provide compliance in accordance with Clause 5(a) and/or Clause 5(b), the data importer agrees to promptly inform 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 affected parts of the Service in accordance with the terms of the Agreement.
3. If the data exporter intends to suspend the transfer of personal data and/or terminate the affected parts of the Service, it shall first provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance (“Cure Period”).
4. In addition, the data exporter and data importer shall reasonably cooperate with each other during the Cure Period to agree what additional safeguards or other measures, if any, may be reasonably required to ensure the data importer's compliance with the Clauses and applicable data protection law.
5. If, after the Cure Period, the data importer has not or cannot cure the non-compliance in accordance with the paragraphs 3 and 4 above, then the data exporter may suspend and/or terminate the affected part of the Service in accordance with the provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by the data exporter prior to suspension or termination).

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 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).
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) inform the government agency that Mailchimp is a processor of the data; (ii) attempt to redirect the agency to request the data directly from Customer; and (iii) 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. 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, Sites, or Service.

UK:

1. For the avoidance of doubt, when European Union law ceases to apply to the UK upon the UK's withdrawal from the European Union and until such time as the UK is deemed to provide adequate protection for personal data (within the meaning of applicable EU Data Protection Law) then to the extend Mailchimp processes (or causes to be processed) any Customer Data protected by EU Data Protection Law applicable to EEA and Switzerland in the United Kingdom, Mailchimp shall process such Customer Data in compliance with the SCCs or any applicable Alternative Transfer Mechanism implemented in accordance with Section 6.3 and 6.4 of this DPA.

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 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, including, without limitation, in the Agreement, 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 November 23, 2020