

Data Processing Addendum

This document outlines the Data Processing Addendums in place with Okta and The Rocket Science Group LLC, operating as Mailchimp. These Addendums are applicable solely to current beta testers of Clipzy. By utilizing the application, you consent to the transfer of your personal data to the United States if you are not already located within its jurisdiction. For access to the Mailchimp Addendum, please refer to page 24. Alternatively, proceed to the subsequent page.

Sincerely,

Jose Moran Urena
Head Developer | Clipzy



DATA PROCESSING ADDENDUM

Based on the General Data Protection Regulation (GDPR) and European Commission Decision 2021/914/EU - Standard Contractual Clauses

This Data Processing Addendum (“DPA”) forms part of the Master Subscription Agreement (or other such titled written or electronic agreement addressing the same subject matter) between Okta and Customer for the purchase of online identity-as-a-service and access management services (including related Okta offline or mobile components) from Okta (identified collectively either as the “Service” or otherwise in the applicable agreement, and hereinafter defined as the “Service”), wherein such agreement is hereinafter defined as the “Agreement,” and whereby this DPA reflects the parties’ agreement with regard to the Processing of Personal Data. Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Okta processes Personal Data for which such Authorized Affiliates qualify as the Controller or a Processor. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In providing the Service to Customer pursuant to the Agreement, Okta may Process Personal Data on behalf of Customer, and the parties agree to comply with the following provisions with respect to any Personal Data.

This DPA consists of distinct parts: (1) this body and its set of definitions and provisions, and (2) the Standard Contractual Clauses and Annexes I, II, III and IV (if applicable). Please note that the Controller-to-Processor and Processor-to-Processor Standard Contractual Clauses are included by reference and their full text, including Annex III and Annex IV addressing respectively data transfers with Switzerland and the United Kingdom, is available via a link in the definitions of this DPA.

INSTRUCTIONS ON HOW TO EXECUTE THIS DPA WITH OKTA

1. This DPA has been pre-signed on behalf of Okta, Inc., as the data importer.
2. To complete this DPA, Customer must complete the information in the signature box and sign on Page 8.
3. Customer must send the completed and signed DPA to Okta either by (1) email, indicating the Customer’s full entity name (as set out on the applicable Okta Order Form or invoice) in the body of the email, to DPA@okta.com; or (2) by completing the DPA digitally, via the link at the following webpage: <https://www.okta.com/trustandcompliance> . Upon receipt of the validly-completed DPA by Okta at either the email address in part (1) or via the web as described in part (2) of the prior sentence, this DPA shall come into effect and legally bind the parties.

APPLICATION OF THIS DPA

If the Customer entity signing this DPA is a party to the Agreement, then this DPA is an addendum to, and forms part of, the Agreement. In such case, the Okta entity (i.e., either Okta, Inc. or a subsidiary of Okta, Inc.) that is party to the Agreement is party to this DPA.



If the Customer entity signing this DPA has executed an Order Form with Okta or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, then this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the Okta entity that is a party to such Order Form is a party to this DPA.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, then this DPA is not valid and therefore is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

DPA DEFINITIONS

“Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the Customer entity signing this Agreement, or with Okta, Inc., as the case may be. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“Authorized Affiliate” means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Service pursuant to the Agreement between Customer and Okta, but has not signed its own Order Form with Okta and is not a "Customer" as defined under the Agreement.

“CCPA” means the California Consumer Privacy Act, California Civil Code sections 1798.100 *et seq.*, as amended by the California Privacy Rights Act of 2020, including any implementing regulations.

“Controller” means the entity which determines the purposes and means of the Processing of Personal Data.

“Controller to Processor Standard Contractual Clauses” means the agreement executed by and between Customer acting as Controller and Okta acting as Processor and included herein, pursuant to the European Commission’s Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. The Controller to Processor Standard Contractual Clauses are currently available [here](#).

“Customer Data” means all electronic data submitted by or on behalf of Customer, or an Authorized Affiliate, to the Service.

“Data Protection Laws and Regulations” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, and the United States and its states, applicable to the Processing of Personal Data under the Agreement.

“Data Subject” means the identified or identifiable person to whom Personal Data relates.

“Deidentified Data” means data that cannot reasonably be used to infer information about, or otherwise be linked to, a Data Subject and where such data is Processed only in accordance with the section “Deidentified Data” of this DPA.



“GDPR” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

“Okta” means the Okta entity which is a party to this DPA, as specified in the section “Application of this DPA” above, being Okta, Inc., a company incorporated in Delaware and its primary address as 100 First Street, San Francisco California 94105, USA, or an Affiliate of Okta, as applicable.

“Okta Group” means Okta and its Affiliates engaged in the Processing of Personal Data.

“Personal Data” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

“Processing” (including its root word, “Process”) means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means the entity which Processes Personal Data on behalf of the Controller.

“Processor to Processor Standard Contractual Clauses” means the agreement executed by and between Customer acting as a Processor acting on behalf of a Controller and Okta acting as a Processor on behalf of Customer pursuant to the European Commission’s Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. The Processor to Processor Standard Contractual Clauses are currently available [here](#).

“Standard Contractual Clauses” means either the Controller to Processor Standard Contractual Clauses or the Processor to Processor Standard Contractual Clauses, as currently available [here](#).

“Sub-processor” means any Processor engaged by Okta or a member of the Okta Group.

“Supervisory Authority” means an independent public authority which is established by an EU Member State pursuant to the GDPR.

“Trust & Compliance Documentation” means the Documentation applicable to the specific Service purchased by Customer, as may be updated periodically, and accessible via Okta’s website at www.okta.com/agreements, or as otherwise made reasonably available by Okta.

DPA TERMS

Okta and the signatory below at the address below (“Customer”) hereby enter into this DPA effective as of the



last signature date below. This DPA is incorporated into and forms part of the Agreement.

1. **Provision of the Service.** Okta provides the Service to Customer under the Agreement. In connection with the Service, the parties anticipate that Okta may Process Customer Data that contains Personal Data relating to Data Subjects.

2. **The Parties' Roles.** The parties agree that with regard to the Processing of Personal Data, Okta acts as Processor on behalf of the Customer, which may act either as a Controller or a Processor, and that Okta or members of the Okta Group will engage Sub-processors pursuant to the requirements of this DPA. For the avoidance of doubt, to the extent Processing of Personal Data is subject to the CCPA, the parties agree that Customer is the "Business" and Okta is the "Service Provider" (as those terms are defined by the CCPA).

3. **Customer Responsibilities.** Customer shall, in its use of the Service, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirements to provide notice to Data Subjects of the use of Okta as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges that its use of the Service will not violate the rights of any Data Subject that has opted-out from sales, or other disclosures of Personal Data, to the extent applicable under the CCPA or other Data Protection Laws and Regulations.

4. **Processing Purposes.** Okta shall keep Personal Data confidential and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Service; and (iii) Processing to comply with other documented, reasonable instructions provided by Customer (for example, via email) where such instructions are consistent with the terms of the Agreement. Okta shall not be required to comply with or observe Customer's instructions if such instructions would violate any Data Protection Laws and Regulations.

5. **Scope of Processing.** The subject-matter of the Processing of Personal Data by Okta is the performance of the Service pursuant to the Agreement and Okta acknowledges that Customer is disclosing or authorizing Okta to collect on Customer's behalf, or is otherwise making available, Personal Data in connection with this Agreement for the limited purposes set out in the Agreement and this DPA, as specified in Annex I. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Annex I to the Standard Contractual Clauses attached to this DPA.

6. **Data Subject Requests.** To the extent legally permitted, Okta shall promptly notify Customer if Okta receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Factoring into account the nature of the Processing, Okta shall assist Customer by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under



Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Service, does not have the ability to address a Data Subject Request, Okta shall, upon Customer's request, provide commercially-reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent that Okta is legally authorized to do so, and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Okta's provision of such assistance.

7. **Okta Personnel.** Okta shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training regarding their responsibilities, and have executed written confidentiality agreements. Okta shall take commercially-reasonable steps to ensure the reliability of any Okta personnel engaged in the Processing of Personal Data. Okta shall ensure that Okta's access to Personal Data is limited to those personnel assisting in the provision of the Service in accordance with the Agreement.

8. **Data Protection Officer.** Members of the Okta Group have appointed a data protection officer. The appointed person may be reached at privacy@okta.com.

9. **Sub-processing.**

9.1 Okta's Sub-processors. Customer has instructed or authorized the use of Sub-processors to assist Okta with respect to the performance of Okta's obligations under the Agreement pursuant to a written contract that binds each Sub-processor to comply with applicable Data Protection Laws and Regulations and with terms no less protective of privacy than the terms in this DPA. Okta shall be liable for the acts and omissions of its Sub-processors to the same extent Okta would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

9.2 List of Okta's Sub-processors. A list of Okta's current Sub-processors, including a description of their processing activities and locations, is made available on Okta's Agreements webpage (accessible via www.okta.com/agreements under the "Trust & Compliance Documentation" link). Customer acknowledges and agrees that (a) Okta's Affiliates may be retained as Sub-processors; and (b) Okta and Okta's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Service. On Okta's Agreements webpage (accessible via www.okta.com/agreements under the "Trust & Compliance Documentation" link), Customer may find a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, to which Customer shall subscribe, and if Customer subscribes, Okta shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to process Personal Data in connection with the provision of the applicable Service.

9.3 Right to object to a new Sub-processor. In order to exercise its right to object to Okta's use of a new Sub-processor, Customer shall notify Okta promptly in writing within ten (10) business days after receipt of Okta's notice in accordance with the mechanism set out above. In the event Customer objects to a new Sub-processor, and that objection is not unreasonable, Okta will use reasonable efforts to make available to Customer a change in the Service or recommend a commercially-reasonable change to Customer's configuration or use of the Service to avoid Processing of Personal Data by the objected-to new Sub-



processor without unreasonably burdening the Customer. If Okta is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those aspects of the Service which cannot be provided by Okta without the use of the objected-to new Sub-processor by providing written notice to Okta. Okta will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Service.

9.4 Sub-processors and the Standard Contractual Clauses. Customer acknowledges and agrees that Okta may engage Sub-processors as described in this section for the fulfilment of Okta's obligations under Clause 9(a) of the Standard Contractual Clauses. The parties agree that the copies of the Sub-processor agreements that must be provided by Okta to Customer pursuant to Clause 9(c) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Okta beforehand to protect business secrets or other confidential information; and, that such copies will be provided by Okta, in a manner to be determined in its discretion, only upon request by Customer.

10. Security Measures. Okta shall maintain appropriate organizational and technical measures for protection of the security (including protection against unauthorized or unlawful Processing, and against unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Customer Data), confidentiality, and integrity of Customer Data, as set forth in Okta's applicable Trust & Compliance Documentation. Okta regularly monitors compliance with these measures. Okta will not materially decrease the overall security of the Service during a subscription term.

11. Third-Party Certifications and Audit Results. Okta has attained the third-party certifications and audit results set forth in the Trust & Compliance Documentation. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Okta shall make available to Customer a copy of Okta's then most recent third-party certifications or audit results, as applicable.

12. Notifications Regarding Customer Data. Okta has in place reasonable and appropriate security incident management policies and procedures, as specified in the Trust & Compliance Documentation and shall notify Customer without undue delay after a breach of security that causes the unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Okta or its Sub-processors, of which Okta becomes aware (hereinafter, a "Customer Data Incident"). Okta shall make reasonable efforts to identify the cause of such Customer Data Incident, and take those steps as Okta deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident, to the extent that the remediation is within Okta's reasonable control. The obligations set forth herein shall not apply to incidents that are caused by either Customer or Customer's Users.

13. Return of Customer Data. Okta shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and time periods specified in the Trust & Compliance Documentation, unless the retention of the data is requested from Okta according to mandatory statutory laws.



14. **Authorized Affiliates.** The parties agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliate(s), thereby establishing a separate DPA between Okta and each such Authorized Affiliate, subject to the provisions of the Agreement. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. An Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Service by Authorized Affiliate(s) must comply with the terms and conditions of the Agreement and any violation thereof by an Authorized Affiliate shall be deemed a violation by Customer.

15. **Communications.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Okta under this DPA, and shall be entitled to transmit and receive any communication in relation to this DPA on behalf of its Authorized Affiliate(s).

16. **Exercise of Rights.** Where an Authorized Affiliate becomes a party to the DPA, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Okta directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA in a combined manner for all of its Authorized Affiliates together, instead of doing so separately for each Authorized Affiliate.

17. **Liability.** Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Okta, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. Okta's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA. Each reference to the DPA herein means this DPA including its Appendices.

18. **GDPR and CCPA Compliance.** Okta will Process Personal Data in accordance with the GDPR and CCPA requirements directly applicable to Okta's provision of the Service. For clarity, to the extent applicable to Okta's provision of the Service, Okta shall: (1) Process Personal Data only as set forth in the Agreement and this DPA; and (2) Process Personal Data in compliance with the GDPR and CCPA. Okta agrees to promptly notify Customer upon becoming aware that Okta can no longer comply with the GDPR or the CCPA, the timing of which notification shall be consistent with applicable legal requirements. Upon Customer's reasonable written notice, Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data to the extent required of Customer under the GDPR and CCPA.



19. **APEC Privacy Recognition for Processors.** Okta has obtained APEC Privacy Recognition for Processors ("PRP") certification and, for the Okta-branded aspects of the Service, shall Process Personal Data submitted to such Service as listed in Okta's PRP certification, which Okta makes available online at <https://www.okta.com/trustandcompliance>. As of the date of this DPA, Okta's PRP certification does not extend to the aspects of the Service branded as 'Customer Identity Cloud' (and which were previously branded as 'Auth0').

20. **EU Cloud Code of Conduct.** Okta has obtained the European Union Cloud Code of Conduct ("EU CCC") privacy certification and, for the Okta-branded aspects of the Service, shall process Personal Data submitted to such Service as listed in Okta's EU CCC certification, which Okta makes available online at <https://www.okta.com/trustandcompliance>. As of the date of this DPA, Okta's EU CCC certification does not extend to aspects of the Service branded as 'Customer Identity Cloud' (and which were previously branded as 'Auth0').

21. **Data Protection Impact Assessment.** Upon Customer's request, Okta shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Service, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Okta. Okta shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this section of this DPA, to the extent required under the GDPR.

22. **Standard Contractual Clauses.** The Standard Contractual Clauses apply to:

- (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Authorized Affiliates and,
- (ii) all Affiliates of Customer established within the European Economic Area, Switzerland and the United Kingdom, which have signed Order Forms for the Service.

For the purpose of the Standard Contractual Clauses the aforementioned entities shall be deemed "data exporters." If necessary to fulfil its legal obligations, Customer may share a copy of the attached Standard Contractual Clauses with Data Subjects.

23. **Customer's Processing Instructions.** This DPA and the Agreement are Customer's complete and final instructions at the time of signature of the Agreement to Okta for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 8.1 of the Standard Contractual Clauses, the following is deemed an instruction by the Customer to process Personal Data:

- (a) Processing in accordance with the Agreement and applicable Order Form(s);
- (b) Processing initiated by Users in their use of the Service and
- (c) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

24. **Audits.** The parties agree that the audits described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: following Customer's written request, and subject to the confidentiality obligations set forth in the Agreement, Okta shall make available to Customer information regarding the Okta Group's compliance with the obligations set forth in this DPA in the form of the third-party



certifications and audits set forth in the Trust & Compliance Documentation, to the extent that Okta makes them generally available to its customers. Customer may contact Okta in accordance with the “Notices” section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Okta for any time expended for any such on-site audit at the Okta Group’s then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Okta shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Okta. Customer shall promptly notify Okta and provide information about any actual or suspected non-compliance discovered during an audit. The provision in this section shall by no means derogate from or materially alter the provisions on audits as specified in the Standard Contractual Clauses.

25. **Data Deletion.** The parties agree that the certification of deletion of Personal Data that is described in Clauses 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Okta to Customer only upon Customer’s request.

26. **Personal Data Restrictions.** To the extent that Personal Data is subject to the CCPA, Okta shall not (1) “sell” or “share” Personal Data, as those terms are defined under the CCPA, (2) retain, use, disclose, or otherwise Process Personal Data for any purpose other than the business purposes specified in the Agreement or Annex I, or as otherwise permitted by the CCPA, or (3) retain, use, disclose, or otherwise Process Personal Data in any manner outside of the direct business relationship between Customer and Okta, or combine any Personal Data with personal data that Okta receives from or on behalf of any third party or collects from Okta’s own interactions with Data Subjects, except as permitted by the Data Protections Laws and Regulations. For clarity, Customer’s use of the Service to combine Personal Data with personal data that Okta receives from third parties and/or collected from Customer’s or Okta’s own interactions with Data Subjects for the purposes of providing the Service and as noted in the Documentation is deemed a combination authorized by Customer.

27. **Deidentified Data.** To the extent Customer discloses or otherwise makes available Deidentified Data to Okta, or to the extent Okta generates Deidentified Data from Personal Data, Okta shall (1) implement technical safeguards that prohibit re-identification of the User to whom the information may pertain; (2) has implemented business processes that specifically prohibit re-identification of the Deidentified Data and prevent the inadvertent release of De-identified Data; and (3) make no attempt to reidentify the Deidentified Data.

28. **Language.** The governing language of this DPA is English. Any Japanese language version of this DPA is for reference purposes only. If there is any conflict between the English and Japanese version, the English version shall prevail.

29. **Order of Precedence.** This DPA is incorporated into and forms part of the Agreement and the Standard Contractual Clauses are incorporated by reference to this DPA. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the parties vis-à-vis each other, in the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control. In the event of a conflict between the terms of the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.



Agreed by Customer:

DocuSigned by:
Signature: Jose Moran Urena
B2B363379CF046F...
By: Jose Moran Urena
Title: Head Developer
Date: February 10, 2024

Agreed by Okta, Inc.:

Signature: Larissa Schwartz
By: Larissa Schwartz
Title: Chief Legal Officer
Date: February 10, 2024



ANNEXES TO THE STANDARD CONTRACTUAL CLAUSES (IF APPLICABLE)

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The entity named as "Customer" in the DPA clipzy

Address: The address for Customer associated with its Okta account or as otherwise specified in the DPA or the Agreement.

Contact person's name, position and contact details: The address for Customer associated with its Okta account or as otherwise specified in the DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: Processing of Personal Data, where such data is Customer Data, for the performance of the identity and access management cloud services upon the instruction of the data exporter in accordance with the terms of the Agreement and the DPA.

Signature and date: By executing the DPA, the data exporter will be deemed to have signed this Annex I.

Role: Controller and/or processor

Data importer(s):

Name: Okta, Inc.

Address: 100 First Street, San Francisco, California 94105, USA

Contact person's name, position and contact details: Lisa Turbis, Data Protection Officer, privacy@okta.com

Activities relevant to the data transferred under these Clauses: Processing of Personal Data, where such data is Customer Data, for the performance of the identity and access management cloud services upon the instruction of the data exporter in accordance with the terms of the Agreement and the DPA.

Signature and date:  (March 1, 2023)
Larissa Schwartz, Chief Legal Officer

Role: Processor on behalf of Customer



B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customers, business partners, and vendors of the data exporter (who are natural persons)
- Employees or contact persons of data exporter customers, business partners, and vendor
- Employees, agents, advisors, contractors, or any user authorized by the data exporter to use the Service (who are natural persons)

Categories of personal data transferred

Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of personal data:

- Identifiers, such as first and last name, ID data, business contact information (company, email, phone, physical business address), and personal contact information (email, cell phone)
- Categories of Personal Data described in subdivision (e) of Section 1798.80 of the CCPA (as defined by this DPA), such as title, position, employer, professional life data, and personal life data (in the form of security questions and answers)
- Internet or other network or device activity details, such as connection data
- Localization data
- Commercial information, such as records of products or services purchased and other transactional data

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Data exporter may submit special categories of data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include Personal Data concerning health information. If applicable, data exporter agrees that it has reviewed and assessed the restrictions and safeguards applied to the special categories of Personal Data, including the measures described in the Trust & Compliance Documentation (as defined by this DPA) and Documentation (as defined in the Agreement), and has determined that such restrictions and safeguards are sufficient.



The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Subject to Customer's use of the Service, Personal Data will be transferred on a continuous basis during the term of the Agreement.

Nature of the processing

Identity and access management and related services pursuant to the Agreement.

Business Purpose(s) of the data transfer and further processing

The objective of Processing of Personal Data by the data importer is the performance of the Service and services pursuant to the Agreement and as instructed by data exporter in its use of the Service.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data exporter may retain Personal Data in the Service for the duration of the Agreement. Personal Data within the Service post-termination of the Agreement will be retained and deleted in accordance with the Documentation.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Sub-processors may only Process Personal Data as necessary for the performance of the Service pursuant to the Agreement and for the duration of the Agreement. Sub-processor information are made available on Okta's 'Agreements' webpage (accessible via www.okta.com/agreements under the "Trust & Compliance Documentation" link).

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.



Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located shall act as competent supervisory authority.



ANNEX II
**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND
ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Okta maintains administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, including Personal Data, as set forth in the Trust & Compliance Documentation (accessible via <https://www.okta.com/trustandcompliance/>). Okta regularly monitors compliance with these safeguards. Okta will not materially decrease the overall security of the Service during a subscription term. Okta's Service is designed to permit data exporter to manage Data Subject Requests without assistance from Okta. If data exporter cannot complete its obligations pursuant to a Data Subject Request without assistance from Okta, then, and as set forth in the section "Data Subject Requests" of the DPA, factoring into account the nature of the Processing, Okta shall assist data exporter by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of data exporter's obligation to respond to a Data Subject Request.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Okta conducts reasonable due diligence and security assessments of Sub-processors, and enters into agreements with Sub-processors that contain provisions similar to or more stringent than those provided for in the Security & Privacy Documentation within Trust & Compliance Documentation. Okta will work directly with Sub-processors, as necessary, to provide assistance to data exporter.



ANNEX III
DATA TRANSFERS FROM SWITZERLAND

In case of any transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland (“Swiss Data Protection Laws”), the following provisions apply:

1. General and specific references in the Standard Contractual Clauses to GDPR, or EU or Member State Law, shall have the same meaning as the equivalent reference in Swiss Data Protection Laws, as applicable.
2. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.
3. Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws.
4. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.



ANNEX IV

DATA TRANSFERS FROM THE UNITED KINGDOM

In case of any transfers of Personal Data from the United Kingdom, the following provisions apply:

This annex provides the addendum that has been issued by the Information Commissioner for parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Where this annex uses capitalized terms that are defined in the DPA, including the Standard Contractual Clauses, those terms shall have the same meaning as in the Standard Contractual Clauses. Other capitalized terms have the meanings provided by the Addendum B.1.0, issued by the Information Commissioner's Office and laid before the United Kingdom Parliament in accordance with section 119A of the Data Protection Act 2018 on February 2, 2022.

Part 1: Tables

Table 1: Parties

As pursuant to Annex IA – List of the Parties of the DPA

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	<p>The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:</p> <p>Date: As pursuant to the effective date of the DPA</p> <p>Reference (if any): The relevant modules of the Addendum EU SCCs are available on Okta's Trust & Compliance Documentation page at https://www.okta.com/trustandcompliance/</p> <p>Other identifier (if any): not applicable</p>
-------------------------	--

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:



Annex 1A: List of Parties: Page 11 of the DPA
Annex 1B: Description of Transfer: Pages 12 to 14 of the DPA
Annex II: Technical and organisational measures, including technical and organisational measures to ensure the security of the data: Page 15 of the DPA
Annex III: The list of Sub-processors is available on Okta's Trust & Compliance Documentation page at https://www.okta.com/trustandcompliance/

Table 4: Terminating this Addendum when the Approved Addendum Changes

Terminating this Addendum when the Approved Addendum changes	<p>Which Parties may terminate this Addendum as set out in section 19 of the Approved Addendum:</p> <p><input checked="" type="checkbox"/> Importer</p> <p><input type="checkbox"/> Exporter</p> <p><input type="checkbox"/> neither Party</p>
---	--

Part 2: Mandatory Clauses

Mandatory Clauses	<p>Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before the United Kingdom Parliament in accordance with section 119A of the Data Protection Act 2018 on February 2, 2022, as it is revised under section 18 of those Mandatory Clauses.</p>
--------------------------	---


Certificate Of Completion

Envelope Id: D3665089B4D84060ACB362D952C04E91	Status: Completed
Subject: Please DocuSign: OKTA-Data Processing Addendum	
Source Envelope:	
Document Pages: 18	Signatures: 1
Certificate Pages: 4	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelope Stamping: Enabled	Okta Contracts
Time Zone: (UTC-08:00) Pacific Time (US & Canada)	100 First St. Plaza, 14th Floor,
	San Francisco, CA 94105
	dpa@okta.com
	IP Address: 68.192.204.220

Record Tracking

Status: Original	Holder: Okta Contracts	Location: DocuSign
2/10/2024 7:00:53 PM	dpa@okta.com	

Signer Events	Signature	Timestamp
---------------	-----------	-----------

Jose Moran Urena	<div>DocuSigned by:  B2B363379CF046F...</div>	Sent: 2/10/2024 7:00:55 PM
jmuofficial@clipzyapp.com		Viewed: 2/10/2024 7:01:22 PM
Head Developer		Signed: 2/10/2024 7:03:13 PM
Clipzy		
Security Level: Email, Account Authentication (None)	Signature Adoption: Pre-selected Style	
	Using IP Address: 68.192.204.220	

Electronic Record and Signature Disclosure:
Accepted: 2/10/2024 7:01:22 PM
ID: c42265ce-31cd-4222-bd42-cbbee496c071

In Person Signer Events	Signature	Timestamp
-------------------------	-----------	-----------

Editor Delivery Events	Status	Timestamp
------------------------	--------	-----------

Agent Delivery Events	Status	Timestamp
-----------------------	--------	-----------

Intermediary Delivery Events	Status	Timestamp
------------------------------	--------	-----------

Certified Delivery Events	Status	Timestamp
---------------------------	--------	-----------

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

Witness Events	Signature	Timestamp
----------------	-----------	-----------

Notary Events	Signature	Timestamp
---------------	-----------	-----------

Envelope Summary Events	Status	Timestamps
-------------------------	--------	------------

Envelope Sent	Hashed/Encrypted	2/10/2024 7:00:55 PM
Certified Delivered	Security Checked	2/10/2024 7:01:22 PM
Signing Complete	Security Checked	2/10/2024 7:03:13 PM
Completed	Security Checked	2/10/2024 7:03:13 PM

Payment Events	Status	Timestamps
----------------	--------	------------

Electronic Record and Signature Disclosure

CONSUMER DISCLOSURE

From time to time, Okta, Inc. (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through your DocuSign, Inc. (DocuSign) Express user account. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by clicking the "I agree" button at the bottom of this document.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. For such copies, as long as you are an authorized user of the DocuSign system you will have the ability to download and print any documents we send to you through your DocuSign user account for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign "Withdraw Consent" form on the signing page of your DocuSign account. This will indicate to us that you have withdrawn your consent to receive required notices and disclosures electronically from us and you will no longer be able to use your DocuSign Express user account to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through your DocuSign user account all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Okta, Inc.:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: jrandall@okta.com

To advise Okta, Inc. of your new e-mail address

To let us know of a change in your e-mail address where we should send notices and disclosures electronically to you, you must send an email message to us at jrandall@okta.com and in the body of such request you must state: your previous e-mail address, your new e-mail address. We do not require any other information from you to change your email address..

In addition, you must notify DocuSign, Inc to arrange for your new email address to be reflected in your DocuSign account by following the process for changing e-mail in DocuSign.

To request paper copies from Okta, Inc.

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an e-mail to jrandall@okta.com and in the body of such request you must state your e-mail address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Okta, Inc.

To inform us that you no longer want to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your DocuSign account, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an e-mail to jrandall@okta.com and in the body of such request you must state your e-mail, full name, US Postal Address, telephone number, and account number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

Operating Systems:	Windows2000 or WindowsXP
Browsers (for SENDERS):	Internet Explorer 6.0 or above
Browsers (for SIGNERS):	Internet Explorer 6.0, Mozilla FireFox 1.0, NetScape 7.2 (or above)
Email:	Access to a valid email account
Screen Resolution:	800 x 600 minimum
Enabled Security Settings:	Allow per session cookies Users accessing the internet behind a Proxy Server must enable HTTP 1.1 settings via proxy connection

** These minimum requirements are subject to change. If these requirements change, we will provide you with an email message at the email address we have on file for you at that time providing you with the revised hardware and software requirements, at which time you will have the right to withdraw your consent.

Acknowledging your access and consent to receive materials electronically

To confirm to us that you can access this information electronically, which will be similar to

other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your future reference and access or that you were able to e-mail this disclosure and consent to an address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, please let us know by clicking the "I agree" button below.

By checking the "I Agree" box, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC CONSUMER DISCLOSURES document; and
- I can print on paper the disclosure or save or send the disclosure to a place where I can print it, for future reference and access; and
- Until or unless I notify Okta, Inc. as described above, I consent to receive from exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by Okta, Inc. during the course of my relationship with you.

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 (i) 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 (ii) 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 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.

“**UK Addendum**” means the [International Data Transfer Addendum](#) (version B1.0) issued by the Information Commissioner’s Office under S.119(A) of the UK Data Protection Act 2018, as updated or amended from time to time.

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 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. 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, within 48 hours of awareness; (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 industry leading standards by independent third party auditors and internal auditors respectively. Upon written request [here](#), 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 by making additional information available regarding its information security program upon Customer's written request, provided that Customer shall not exercise this right more than once per calendar year. Customers may submit their requests [here](#).

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 EEA Data Transfers. To the extent that Mailchimp is a recipient of Customer Data protected by GDPR in a country outside of EEA 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 such Customer Data in compliance with the SCCs, which shall be incorporated into and form an integral part of this DPA.

6.4 UK Data Transfers. With respect to transfers to which the UK Data Protection Laws apply, the SCCs shall apply and shall be deemed amended as specified by the UK Addendum. The UK Addendum shall be deemed executed by the parties and incorporated into and form an integral part of this DPA. In addition: Tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annexes I and II of the relevant SCCs; and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

6.5 Swiss Data Transfers. With respect to transfers to which the Swiss DPA apply, the SCCs shall apply in accordance with Section 6.3 with the following modifications: (i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA; (ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA; (iii) references to "EU", "Union" and "Member State law" shall be replaced with "Switzerland"; (iv) Clause 13(a) and Part C of Annex II shall be deleted; (v) references to the "competent supervisory authority" and "competent courts" shall be replaced with "the Swiss Federal Data Protection and Information Commissioner" and "relevant courts in Switzerland"; (vi) Clause 17 shall be replaced to state "The Clauses are governed by the laws of Switzerland"; and (vii) Clause 18 shall be replaced to state "Any dispute arising from these Clauses shall be resolved by the applicable courts of Switzerland. The parties agree to submit themselves to the jurisdiction of such courts".

6.6 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.

6.7 Alternative transfer mechanism. 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 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).

(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 Agreement.

(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 information permissible when responding to the agency or authority based on a reasonable 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 August 1, 2023