DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "***DPA***"), dated as of the date of the last signature below (the "***DPA Effective Date***"), forms part of dmarcian's Terms of Service, which are available at https://dmarcian.com/terms-of-service/, entered into by and between dmarcian, Inc. ("***dmarcian***") and _____ ("***Customer***") under which dmarcian provides certain Domain Message Authentication, Reporting & Conformance (DMARC) services ("***Services***") to Customer, unless Customer has entered into a superseding written master subscription agreement with dmarcian regarding the Services, in which case, this DPA forms a part of such written agreement (in either case, the "**Agreement**"). All capitalized terms not defined herein shall have the meaning set forth in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

1. **Effectiveness**

a. Scope. This DPA shall only apply to the extent required by Data Protection Laws with regard to the relevant Customer Personal Data. In case of any conflict between the provisions of the Agreement and the provisions of this DPA with respect to such Processing, the provisions of this DPA shall apply.

b. Termination. This DPA will terminate upon the earliest of: (i) termination of the Agreement (and without prejudice to the survival of accrued rights and liabilities of the parties and any obligations of the parties which either expressly or by implication survive termination); (ii) as earlier terminated pursuant to the terms of this DPA; or (iii) as agreed by the parties in writing. Upon termination of the Agreement, Customer acknowledges and agrees that it is Customer's responsibility to stop sending any Customer data, including Customer Personal Data, to dmarcian by updating Customer's DNS records and/or terminating forwarding of DMARC data to dmarcian.

2. **Definitions.** As used in this DPA:

"***Australian Data Protection Laws"*** means (i) the Privacy Act 1988, including the 'Australian Privacy Principles' that form part of that Act; and (ii) all other Australian laws applicable in respect of the processing of Personal Data.

"***Customer Personal Data***" means Personal Data received by dmarcian from or on behalf of Customer pursuant to or in connection with the Agreement that is covered by Data Protection Laws.

"***Controller***" means an entity that determines the purposes and means of the Processing of Personal Data.

"***Data Protection Laws***" means the data privacy and security laws and regulations of any jurisdiction applicable to the Processing of Customer Personal Data under the Agreement including, in each case to the extent applicable, European Data Protection Laws, United States Data Protection Laws, Australian Data Protection Laws, and New Zealand Data Protection Laws.

"***Data Subject***" means the identified or identifiable natural person who is the subject of Personal Data.

"***European Data Protection Laws***" means, in each case to the extent applicable: (a) the EU General Data Protection Regulation 2016/679 ("***GDPR***"); (b) the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("***UK GDPR***"), the Data Protection Act of 2018, and all other laws relating to data protection, the processing of personal data, privacy, or electronic communications in force from time to time in the United Kingdom (collectively, "***UK Data Protection Laws***"); (c) the Swiss Federal Act on Data Protection ("***Swiss FADP***"); and (d) any other applicable law, rule, or regulation related to the protection of Customer Personal Data in the European Economic Area, United Kingdom, or Switzerland that is already in force or that will come into force during the term of this DPA.

"***New Zealand Data Protection Laws***" means the Privacy Act 2020 and any other New Zealand laws and regulations applicable to Personal Data.

"***Personal Data***" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, including, but not

limited to, any information that is defined as "personally identifiable information," "personal information," "personal data," or other similar term under Data Protection Laws.

"***Process***" means any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, alignment, combination, restriction, erasure, destruction or disclosure by transmission, dissemination or otherwise making available.

"***Processor***" means an entity that Processes Personal Data on behalf of a Controller.

"***Security Incident***" means a breach of dmarcian's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data in dmarcian's possession, custody, or control. A Security Incident does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

"***Standard Contractual Clauses***" means, as applicable, Module Two (Transfer controller to processor) or Module Three (Transfer processor to processor) of the standard contractual clauses approved by the European Commission's implementing decision (C(2021)3972) of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/678 or the European Parliament and of the Council (available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en), as supplemented or modified by **Appendix 3**.

"***Subprocessor***" means any Processor appointed by dmarcian in connection with the Processing of Customer Personal Data by dmarcian under the Agreement.

"***Supervisory Authority***" means an independent competent public authority established or recognized under Data Protection Laws.

"***United States Data Protection Laws***" means, in each case to the extent applicable: (a) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, when effective, and its implementing regulations (collectively, "***CCPA***"); (b) the Virginia Consumer Data Protection Act ("***VCPDA***"), when effective; (c) the Colorado Privacy Act and its implementing regulations ("***CPA***"), when effective; (d) the Utah Consumer Privacy Act ("***UCPA***"), when effective; (e) Connecticut SB6, An Act Concerning Personal Data Privacy and Online Monitoring ("***CTDPA***"); and (f) any other applicable law or regulation related to the protection of Customer Personal Data in the United States that is already in force or that will come into force during the term of this DPA.

3. Processing of Personal Data

a. Roles of the Parties. The parties acknowledge and agree that, as between the parties, with regard to the Processing of Customer Personal Data under the Agreement, Customer is a Controller and dmarcian is a Processor. In some circumstances, the parties acknowledge that Customer may be acting as a Processor to a third-party Controller in respect of Customer Personal Data, in which case dmarcian will remain a Processor with respect to the Customer. Each party will comply with the obligations applicable to it in such role under Data Protection Laws with respect to the Processing of Customer Personal Data.

b. Customer Instructions. dmarcian will Process Customer Personal Data only in accordance with Customer's documented instructions unless otherwise required by applicable law, in which case dmarcian will inform Customer of such Processing unless notification is prohibited by applicable law. Customer hereby instructs dmarcian to Process Customer Personal Data: (i) to provide the Services to Customer; (ii) to perform its obligations and exercise its rights under the Agreement and this DPA; and (iii) as necessary to prevent or address technical problems with the Services. dmarcian will notify Customer if, in its opinion, an instruction of Customer infringes upon Data Protection Laws. Customer's instructions for the Processing of Customer Personal Data shall comply with Data Protection Laws. Customer shall be responsible for: (A) giving adequate notice and making all appropriate disclosures to Data Subjects regarding

Customer's use and disclosure and dmarcian's Processing of Customer Personal Data; and (B) obtaining all necessary rights, and, where applicable, all appropriate and valid consents to disclose such Customer Personal Data to dmarcian to permit the Processing of such Customer Personal Data by dmarcian for the purposes of performing dmarcian's obligations under the Agreement or as may be required by Data Protection Laws. Customer shall notify dmarcian of any changes in, or revocation of, the permission to use, disclose, or otherwise Process Customer Personal Data that would impact dmarcian's ability to comply with the Agreement, this DPA, or Data Protection Laws.

c. Details of Processing. The parties acknowledge and agree that the nature and purpose of the Processing of Customer Personal Data, the types of Customer Personal Data Processed, the categories of Data Subjects, and other details regarding the Processing of Customer Personal Data are as set forth in **Appendix 1**.

d. Processing Subject to the CCPA. As used in this Section 3(d), the terms "Sell," "Share," "Business Purpose," and "Commercial Purpose" shall have the meanings given in the CCPA and "Personal Information" shall mean any personal information (as defined in the CCPA) contained in Customer Personal Data. dmarcian will not: (i) Sell or Share any Personal Information; (ii) retain, use, or disclose any Personal Information (A) for any purpose other than for the Business Purposes specified in the Agreement, including for any Commercial Purpose other than the Business Purposes specified in the Agreement, or as otherwise permitted by the CCPA, or (B) outside of the direct business relationship between Customer and dmarcian; or (iii) combine Personal Information received from, or on behalf of, Customer with Personal Data received from or on behalf of any third party, or collected from dmarcian's own interaction with Data Subjects, except to perform any Business Purpose permitted by the CCPA. dmarcian hereby certifies that it understands the foregoing restrictions under this Section 3(d) and will comply with them. The parties acknowledge that the Personal Information disclosed by Customer to dmarcian is provided to dmarcian only for the limited and specified purposes set forth in the Agreement and this DPA. dmarcian will comply with applicable obligations under the CCPA and provide the same level of privacy protection to Personal Information as is required by the CCPA. Customer has the right to take reasonable and appropriate steps to help ensure that dmarcian uses the Personal Information transferred in a manner consistent with Customer's obligations under the CCPA by exercising Customer's audit rights in Section 8. dmarcian will notify Customer if it makes a determination that dmarcian can no longer meet its obligations under the CCPA. If dmarcian notifies Customer of unauthorized use of Personal Information, including under the foregoing sentence, Customer will have the right to take reasonable and appropriate steps to stop and remediate such unauthorized use by limiting the Personal Information shared with dmarcian, terminating the portion of the Agreement relevant to such unauthorized use, or such other steps mutually agreed between the parties in writing.

4. dmarcian Personnel. dmarcian restricts its personnel from Processing Customer Personal Data without authorization by dmarcian and will limit the Processing to that which is needed for the specific individual's job duties in connection with dmarcian's provision of the Services under the Agreement. dmarcian will impose appropriate contractual obligations on its personnel, including relevant obligations regarding confidentiality, data protection, and data security.

5. **Data Subject Rights.** dmarcian will, taking into account the nature of the Processing of Customer Personal Data and the functionality of the Services, provide reasonable assistance to Customer by appropriate technical and organizational measures, insofar as this is possible, as necessary for Customer to fulfill its obligations under Data Protection Laws to respond to requests by Data Subjects to exercise their rights under Data Protection Laws. dmarcian reserves the right to charge Customer on a time and materials basis in the event that dmarcian considers that such assistance is onerous, complex, frequent, or time consuming. If dmarcian receives a request from a Data Subject under any Data Protection Laws with respect to Customer Personal Data, dmarcian will advise the Data Subject to submit the request to Customer and Customer will be responsible for responding to any such request.

6. Subprocessors. dmarcian may engage such Subprocessors as dmarcian considers reasonably appropriate for the Processing of Customer Personal Data. A complete list of dmarcian's current Subprocessors, including their functions and locations, is set forth in **Appendix 4** and may be updated by dmarcian from time to time in accordance with this DPA. dmarcian shall notify Customer of the addition or replacement of any Subprocessor at least 30 days prior to engagement and Customer may, on reasonable grounds, object to a new or replaced Subprocessor by notifying dmarcian in writing within 30 days of receipt of dmarcian's notification, giving reasons for Customer's objection. Upon receiving such objection, dmarcian shall: (a) work with Customer in good faith to make available a commercially reasonable change in

the provision of the Services which avoids the use of that proposed Subprocessor; and (b) where such change cannot be made within 30 days of dmarcian's receipt of Customer's notice, Customer may by written notice to dmarcian with immediate effect terminate the portion of the Agreement or any relevant Order Form to the extent that it relates to the Services which require the use of the proposed Subprocessor. This termination right is Customer's sole and exclusive remedy to Customer's objection of any Subprocessor appointed by dmarcian. When engaging any Subprocessor, dmarcian will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in this DPA with respect to Customer Personal Data. dmarcian shall be liable for the acts and omissions of the Subprocessor to the extent dmarcian would be liable under the Agreement and this DPA.

7. **Security.**

a. Security Measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, dmarcian shall implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk, in accordance with the security standards in **Appendix 2** (the "***Security Measures***"). Customer acknowledges that the Security Measures may be updated from time to time upon reasonable notice to Customer to reflect process improvements or changing practices, provided that the modifications will not materially decrease dmarcian's security obligations hereunder.

b. Security Incidents. Upon becoming aware of a confirmed Security Incident, dmarcian will: (i) notify Customer of the Security Incident without undue delay after becoming aware of the Security Incident, but in no case later than 48 hours; and (ii) take reasonable steps to identify the cause of such Security Incident, minimize harm, and prevent a recurrence. dmarcian will take reasonable steps to provide Customer with information available to dmarcian that Customer may reasonably require to comply with its obligations under Data Protection Laws. dmarcian's notification of or response to a Security Incident under this Section 7(b) will not be construed as an acknowledgement by dmarcian of any fault or liability with respect to the Security Incident.

c. Customer Responsibilities. Customer agrees that, without limitation of dmarcian's obligations under this Section 7, Customer is solely responsible for its use of the Services, including: (i) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data; and (b) securing any account authentication credentials, systems, and devices Customer uses to access or connect to the Services, where applicable. Without limiting dmarcian's obligations hereunder, Customer is responsible for reviewing the information made available by dmarcian relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws.

8. **Assessments and Prior Consultations.** In the event that Data Protection Laws require Customer to conduct a data protection impact assessment, transfer impact assessment, or prior consultation with a Supervisory Authority in connection with dmarcian's Processing of Customer Personal Data, following written request from Customer, dmarcian shall use reasonable commercial efforts to provide relevant information and assistance to Customer to fulfil such request, taking into account the nature of dmarcian's Processing of Customer Personal Data and the information available to dmarcian. dmarcian reserves the right to charge Customer on a time and materials basis in the event that dmarcian considers that such assistance is onerous, complex, frequent, or time consuming.

9. **Return or Destruction of Customer Personal Data.** Following termination or expiration of the Agreement, dmarcian shall, at Customer's option, delete or return Customer Personal Data and all copies to Customer, except as required by applicable law. If dmarcian retains Customer Personal Data pursuant to applicable law, dmarcian agrees that all such Customer Personal Data will continue to be protected in accordance with this DPA.

10. **Audit**

a. Report on Compliance. At Customer's written request, dmarcian will provide Customer with all information reasonably necessary for Customer to verify dmarcian's compliance with the security obligations under this DPA. The information will constitute dmarcian Confidential Information under the confidentiality provisions of the Agreement or a non-disclosure agreement executed by the parties. dmarcian shall allow for and contribute to audits,

including inspections, by Customer or an auditor mandated by Customer in relation to the Processing of the Customer Personal Data by dmarcian or any Subprocessor in accordance with the provisions of this Section 10.

b. Applicability of this Section. Customer's information and audit rights only arise under Section 10(a) hereof to the extent that the Agreement does not otherwise provide information and audit rights meeting the relevant requirements of Data Protection Laws.

c. Audit Procedure. An audit shall be conducted in accordance with and subject to the limitations of Section 6(c) (Security Audits) of the Agreement, provided however that: (i) an audit outside normal business hours shall be permitted if the audit or inspection shall be conducted on an emergency basis and where Customer has given dmarcian prior written notice of such emergency audit; and (ii) no limitation with respect to the frequency of audits conducted shall apply to any additional audits or inspections which Customer is required or requested to carry out by a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws, and where Customer has identified its concerns or the relevant requirement in its notice to dmarcian of the audit or inspection.

11. **International Transfer of Data**.

a. Data Processing Facilities. dmarcian may, subject to Sections 11(b) and 11(c), Process Customer Personal Data in the United States or anywhere dmarcian or its Subprocessors maintains facilities. Customer is responsible for ensuring that its use of the Services complies with any cross-border data transfer restrictions of Data Protection Laws.

b. European Transfers. If Customer transfers Customer Personal Data to dmarcian that is subject to European Data Protection Laws, and such transfer is not subject to an alternative adequate transfer mechanism under European Data Protection Laws or otherwise exempt from cross-border transfer restrictions, then Customer (as "data exporter") and dmarcian (as "data importer") agree that the applicable terms of the Standard Contractual Clauses shall apply to and govern such transfer and are hereby incorporated herein by reference. In furtherance of the foregoing, the parties agree that: (i) the execution of this DPA shall constitute execution of the applicable Standard Contractual Clauses as of the DPA Effective Date; (ii) the relevant selections, terms, and modifications set forth in **Appendix 3** shall apply, as applicable; and (iii) the Standard Contractual Clauses shall automatically terminate once the Customer Personal Data transfer governed thereby becomes lawful under European Data Protection Laws in the absence of such Standard Contractual Clauses on any other basis.

c. Other Jurisdictions. If Customer transfers Customer Personal Data to dmarcian that is subject to Data Protection Laws other than European Data Protection Laws which require the parties to enter into standard contractual clauses to ensure the protection of the transferred Customer Personal Data, and the transfer is not subject to an alternative adequate transfer mechanism under Data Protection Laws or otherwise exempt from cross-border transfer restrictions, then the parties agree that the applicable terms of any standard contractual clauses approved or adopted by the relevant Supervisory Authority pursuant to such Data Protection Laws shall automatically apply to such transfer and, as applicable, shall be completed on a mutatis mutandis basis to the completion of the Standard Contractual Clauses as described in Section 11(b).

12. **Limitation of Liability**. Each party's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement. For the avoidance of doubt, dmarcian's total liability for all claims from the Customer or any third party (other than Data Subject) arising out of or related to the Agreement and this DPA shall apply in the aggregate for all claims under both the Agreement and this DPA.

13. **Jurisdiction and Governing Law**. Except as otherwise provided in this DPA, the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.

[SIGNATURE PAGE FOLLOWS]

In Witness Whereof, the duly authorized representatives of dmarcian and Customer have executed this DPA as of the DPA Effective Date.

dmarcian, Inc.

Signature: _____

Name: _____

Position/Title: _____

Date: _____

Customer: _____

Signature: _____

Name: _____

Position/Title: _____

Date: _____

Address: _____

_____

_____

Privacy Contact: _____

_____

_____

Governing Law and Forum for SCCs: _____

APPENDIX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

1. Parties

Customer Details	**Name:** As set forth in the introductory paragraph of the DPA **Role:** Controller and Data Exporter **Address:** As set forth in the signature block of the DPA **Contact person's name, position and contact details:** As set forth in the signature block of the DPA **Signature and date**: The signature in the Addendum shall satisfy the signature requirement for the Standard Contractual Clauses.
dmarcian Details	**Name:** dmarcian, Inc. **Role:** Processor and Data Importer **Address:** P.O. Box 1007 Brevard, NC 28712, USA **Contact person's name, position and contact details:** Data Privacy Officer, privacy@dmarcian.com **Signature and date**: The signature in the Addendum shall satisfy the signature requirement for the Standard Contractual Clauses.

2. Subject matter and duration of the Processing of Customer Personal Data

dmarcian provides tools and services for Domain-based Message Authentication, Reporting, and Conformance (DMARC) policy configuration, monitoring email authentication and delivery, analyzing DMARC reports, and assisting in the remediation of email authentication issues. dmarcian's services are aimed at helping organizations improve their email security posture and protect their domains from being used in phishing and spoofing attacks. In order to provide these tools and services, dmarcian will process Customer Personal Data on an ongoing basis for the term of the Agreement.

3. Nature and purpose of the Processing of Customer Personal Data

dmarcian visualizes aggregate DMARC data and presents it in an easy-to-understand format to aid customers in the implementation of the DMARC email security protocol. XML files delivered by email service providers are ingested and presented in a user friendly format.

4. The categories of Data Subjects to whom Customer Personal Data relates

Customer's employees.

5. The categories of Customer Personal Data

IP addresses and email addresses.

6. The sensitive data included in Customer Personal Data

No sensitive data is expected to be exchanged by the parties.

7. The frequency of Customer's transfer of Customer Personal Data to dmarcian

On an ongoing and continuous basis for the term of the Agreement.

8. The period for which Customer Personal Data will be retained, or, if that is not possible, the criteria used to determine that period

On a continuous basis for the term of the Agreement.

9. For transfers to Subprocessors, the subject matter, nature and duration of the Processing of Customer Personal Data

See Appendix 4

APPENDIX 2: SECURITY MEASURES

With respect to Customer Personal Data transferred to or received by dmarcian under the Agreement, dmarcian has implemented, and will maintain, a comprehensive written information security program ("**Information Security Program**") that includes appropriate administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of Customer Personal Data. In particular, the Information Security Program will include the following safeguards where appropriate or necessary to ensure the protection of Customer Personal Data:

1. **Access Controls** – Policies, procedures, and physical and technical controls: (a) to limit physical access to its information systems and the facility or facilities in which they are housed to properly authorized persons; (b) to ensure that all members of its workforce who require access to Customer Personal Data have appropriately controlled access, and to prevent those workforce members and others who should not have access from obtaining access; (c) to authenticate and permit access only to authorized individuals and to prevent members of its workforce from providing Customer Personal Data or information relating thereto to unauthorized individuals; and (d) to reasonably encrypt Customer Personal Data where appropriate.

2. **Security Awareness and Training** – A security awareness and training program for all relevant members of dmarcian's workforce (including management), which includes training on how to implement and comply with its Information Security Program.

3. **Security Incident Procedures** – Policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect attempted attacks on or intrusions into Customer Personal Data or information systems relating thereto, and procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes.

4. **Contingency Planning** – Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages Customer Personal Data or systems that contain Customer Personal Data, including a data backup plan and a disaster recovery plan.

5. **Device and Media Controls** – Policies and procedures on hardware and electronic media that contain Customer Personal Data, and the movement of these items, including policies and procedures to address the final disposition of Customer Personal Data, or the hardware or electronic media on which it is stored, and procedures for removal of Customer Personal Data from electronic media before the media are made available for re-use.

6. **Audit Controls** – Hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements and compliance therewith.

7. **Data Integrity** – Policies and procedures to ensure the confidentiality, integrity, and availability of Customer Personal Data and protect it from disclosure, improper alteration, or destruction.

8. **Storage and Transmission Security** – Technical security measures to guard against unauthorized access to Customer Personal Data that is being transmitted over an electronic communications network, including a mechanism to encrypt Customer Personal Data in electronic form while in transit and in storage on networks or systems to which unauthorized individuals may have access.

9. **Assigned Security Responsibility** – dmarcian will designate a security official responsible for the development, implementation, and maintenance of its Information Security Program. dmarcian will inform the Customer as to the person responsible for security upon request.

10. **Storage Media** – Policies and procedures to ensure that prior to any storage media containing Customer Personal Data being assigned, allocated, or reallocated to another user, or prior to such storage media being permanently

removed from a facility, dmarcian will delete such Customer Personal Data from both a physical and logical perspective, such that the media contains no residual data, or if necessary physically destroy such storage media. dmarcian will maintain an auditable program implementing the disposal and destruction requirements set forth in this section for all storage media containing Customer Personal Data.

11. **Testing** – dmarcian will regularly test the key controls, systems, and procedures of its Information Security Program to ensure that they are properly implemented and effective in addressing the threats and risks identified. dmarcian will conduct an annual independent audit of their controls and effectiveness (SOC2 or ISO 27001). dmarcian will monitor their effectiveness of technical security controls through annual penetration test performed by an independent company.

12. **Adjust the Program** – The specifications provided herein apply as of the DPA Effective Date. dmarcian will monitor, evaluate, and adjust, as appropriate, the Information Security Program in light of any relevant changes in technology or security standards, the sensitivity of the Customer Personal Data, internal or external threats to dmarcian or the Customer Personal Data, and dmarcian's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems. In light of the foregoing, the Information Security Program is subject to change; provided, however, that any such update will not materially diminish the applicable information security protections applicable to Customer Personal Data.

***

APPENDIX 3: STANDARD CONTRACTUAL CLAUSES

1. **Application of Modules**. If Customer is acting as a Controller with respect to Customer Personal Data, "Module Two: Transfer controller to processor" of the Standard Contractual Clauses shall apply. If Customer is acting as a Processor to a third-party Controller with respect to Customer Personal Data, dmarcian is a sub-Processor and "Module Three: Transfer processor to processor" of the Standard Contractual Clauses shall apply.

2. **Sections I-V**. The parties agree to the following selections in Sections I-IV the Standard Contractual Clauses: (a) the parties select Option 2 in Clause 9(a) and the specified time period shall be the notification time period set forth in Section 6 of the DPA; (b) the optional language in Clause 11(a) is omitted; (c) the parties select Option 1 in Clause 17 and the governing law is as set forth in the "Governing Law and Forum for SCCs" field in the signature block of the DPA; and (d) in Clause 18(b), the parties select the courts in the country that is set forth in the "Governing Law and Forum for SCCs" field in the signature block of the DPA.

3. **Annexes**. The name, address, contact details, activities relevant to the transfer, and role of the parties set forth in the Agreement and the DPA shall be used to complete Annex I.A. of the Standard Contractual Clauses. The information set forth in **Appendix 1** to the DPA shall be used to complete Annex I.B. of the Standard Contractual Clauses. The competent supervisory authority in Annex I.C. of the Standard Contractual Clauses shall be the relevant supervisory authority determined by Clause 13 and the GDPR, unless otherwise set forth in Sections 5 or 6 of this **Appendix 3**. If such determination is not clear, then the competent supervisory authority shall be the Irish Data Protection Authority. The technical and organizational measures in Annex II of the Standard Contractual Clauses shall be the measures set forth in **Appendix 2** to the DPA. The information set forth in **Appendix 4** to the DPA shall be used to complete Annex III of the Standard Contractual Clauses.

4. **Supplemental Business-Related Clauses**. In accordance with Clause 2 of the Standard Contractual Clauses, the parties wish to supplement the Standard Contractual Clauses with business-related clauses, which shall neither be interpreted nor applied in such a way as to contradict the Standard Contractual Clauses (whether directly or indirectly) or to prejudice the fundamental rights and freedoms of Data Subjects. dmarcian and Customer therefore agree that the applicable terms of the Agreement and the DPA shall apply if, and to the extent that, they are permitted under the Standard Contractual Clauses, including without limitation the following:

   a. Instructions. The instructions described in Clause 8.1 are set forth in Section 3(b) of the DPA.
   b. Protection of Confidentiality. In the event a Data Subject requests a copy of the Standard Contractual Clauses or the DPA under Clause 8.3, Customer shall make all redactions reasonably necessary to protect business secrets or confidential information of dmarcian.
   c. Deletion or Return. Deletion or return of Customer Personal Data by dmarcian under the Standard Contractual Clauses shall be governed by Section 9 of the DPA. Certification of deletion of Customer Personal Data under Clause 8.5 or Clause 16(d) will be provided by dmarcian upon the written request of Customer.
   d. Onward Transfers. dmarcian shall be deemed in compliance with Clause 8.8 to the extent such onward transfers occur in accordance with Article 4 of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
   e. Audits and Certifications. Any information requests or audits provided for in Clause 8.9 shall be fulfilled in accordance with Section 10 of the DPA.
   f. Liability. The relevant terms of the Agreement which govern indemnification or limitation of liability shall apply to dmarcian's liability under Clauses 12(a), 12(d), and 12(f).
   g. Termination. The relevant terms of the Agreement which govern termination shall apply to a termination pursuant to Clauses 14(f) or 16.

5. **Transfers from the United Kingdom**. If Customer transfers Customer Personal Data to dmarcian that is subject to UK Data Protection Laws, the parties acknowledge and agree that: (a) the template addendum issued by the Information Commissioner's Office of the United Kingdom and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 (available at:

https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf), as it may be revised from time to time by the Information Commissioner's Office (the "***UK DPA***") shall be incorporated by reference herein; (b) the UK DPA shall apply to and modify the Standard Contractual Clauses solely to the extent that UK Data Protection Laws apply to Customer's Processing when making the transfer; (c) the information required to be set forth in "Part 1: Tables" of the UK DPA shall be completed using the information provided in this **Appendix 3** and the DPA; and (d) either party may end the UK DPA in accordance with section 19 thereof.

6. **Transfers from Switzerland.** If Customer transfers Customer Personal Data to dmarcian that is subject to the Swiss FADP, the following modifications shall apply to the Standard Contractual Clauses to the extent that the Swiss FADP applies to Customer's Processing when making that transfer: (a) the term "member state" as used in the Standard Contractual Clauses shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from suing for their rights in their place of habitual residence in accordance with Clause 18(c) of the Standard Contractual Clauses; (b) the Standard Contractual Clauses shall also protect the data of legal entities until the entry into force of the revised Swiss FADP on or about 1 January 2023; (c) references to the GDPR or other governing law contained in the Standard Contractual Clauses shall also be interpreted to include the Swiss FADP; and (d) the parties agree that the supervisory authority as indicated in Annex I.C of the Standard Contractual Clauses shall be the Swiss Federal Data Protection and Information Commissioner.

***

APPENDIX 4: SUBPROCESSORS

Name	Purpose	Location	Privacy Contact	DPA
Google Cloud Platform	Cloud infrastructure	USA: (Iowa); EU: (Belgium); APAC: (Taiwan); Japan: (Tokyo); Cisco EU (Germany); AUS (Sydney) – depending on Customer's choice of its dmarcian account hosting	https://cloud.google.com/contact legal-notices@google.com	https://cloud.google.com/terms/data-processing-addendum
Help Scout	Customer support management desk	USA	177 Huntington Ave, Ste 1703 PMB 78505 Boston, MA 02115-3153, USA Attn: Privacy Agent	https://www.helpscout.com/company/legal/dpa/
Slack	Internal communication	USA	dpo@slack.com	https://slack.com/terms-of-service/data-processing
Google	Productivity software suite	USA	legal-notices@google.com	https://business.safety.google/processorterms/
Pipedrive	Customer relationship management	USA, EU	490 1st Ave South, Suite 800 St. Petersburg, FL 33701, USA Attn: DPO dpo@pipedrive.com	https://www-cms.pipedriveassets.com/documents/Data-Processing-Addendum-Mar_2022.pdf
Twilio	Email delivery provider	USA, Ireland, Australia	101 Spear Street, 5th Floor, San Francisco, California, 94105, USA Attn: DPO privacy@twilio.com	https://www.twilio.com/en-us/legal/data-protection-addendum
Xero	Billing management	USA	1615 Platte Street, Floor 4, Denver, CO 80202, USA Attn: Privacy	https://www.xero.com/us/legal/terms/data-processing/
Panda Doc	Contract review and signature	USA	3739 Balboa St., #1083 San Francisco, CA 94121, USA Attn: Director of Legal and Compliance privacyteam@pandadoc.com	https://public-site.marketing.pandadoc-static.com/app/uploads/PandaDoc-DPA-for-Customers-v22.2-Pre-Signed-Public-Facing.pdf
Chargebee	Credit card processing	USA, EU	909 Rose Avenue, Suite 610, North Bethesda, MD 20852 Attn: Privacy privacy@chargebee.com	https://www.chargebee.com/privacy/dpa/
Crisp	Business messaging platform	EU	dpo@crisp.chat	Not publicly available but see https://help.crisp.chat/en/article/whats-crisp-eu-gdpr-compliance-status-nhv54c/
Intuit	Billing management	USA, Ireland and AU	https://www.intuit.com/privacy/ hrconnect@intuit.com	https://www.dataprivacyframework.gov/s/
Syft	Billing Management	USA	https://www.syftanalytics.com/privacy-policy	legal@syftanalytics.com