Teraswitch Data Processing Addendum

THIS DATA PROCESSING ADDENDUM ("**DPA**") is entered into as of the effective date of the Agreement by and between: (1) Teraswitch, Inc., a Commonwealth of Pennsylvania corporation with its principal business address at 30 Isabella Street, First Floor, Pittsburgh, PA 15212 ("**Teraswitch**"); and (2) the entity or other person that is a counterparty to the Agreement (as defined below) into which this DPA is incorporated and forms a part ("**Customer**"), together the "**Parties**" and each a "**Party**".

1. INTERPRETATION

1.1 In this DPA, the following terms shall have the meanings set out in this Section 1, unless expressly stated otherwise:

(a) "**Agreement**" has the meaning given to the term in the Teraswitch Terms of Service as accepted by Customer, or any other agreement entered into by the Parties that provides that this Addendum will be incorporated therein by reference.

(b) "**Alternative Transfer Mechanism**" means a transfer mechanism, other than SCCs, that enables the lawful disclosure, grant of access, or other transfer of Customer Personal Data that would otherwise have constituted a Restricted Transfer in accordance with Applicable Data Protection Laws (including, as and where applicable, the EU-U.S. Data Privacy Framework, the UK Extension thereto and/or Swiss–U.S. Data Privacy Framework).

(c) "**Applicable Data Protection Laws**" means the privacy, data protection, and data security laws and regulations of any jurisdiction applicable to Teraswitch's Processing of Customer Personal Data under the Agreement (including, as and where applicable, the GDPR, FADP and/or the State Privacy Laws).

(d) "**Controller**" means the natural or legal person that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(e) "**Customer Personal Data**" means any Content Data that constitutes or contains Personal Data and that Teraswitch or its Sub-Processors Process on behalf of Customer to perform the Services. For the avoidance of doubt, Customer Personal Data does not include Usage Data.

(f) "**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

(g) "**Data Subject Request**" means the exercise by a Data Subject of its rights in accordance with Applicable Data Protection Laws with respect to Customer Personal Data and the Processing thereof.

(h) "**FADP**" means the Swiss Federal Act on Data Protection of 25 September 2020.

(i) "**GDPR**" means, as and where applicable to Processing concerned: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**"); and/or (ii) the EU GDPR as it forms part of UK law (as amended from time to time) ("**UK GDPR**").

(j) "**Personal Data**" means "personal data," "personal information," "personally identifiable information," or a similar term defined in Applicable Data Protection Laws.

(k) "**Personal Data Breach**" means a breach of Teraswitch's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or

access to, Customer Personal Data in Teraswitch's possession, custody, or control. For clarity, Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data (such as unsuccessful login attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems).

(l) "**Personnel**" means a person's employees, contractors, consultants, agents, and other staff.

(m) "**Process**," and grammatical inflections thereof, means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means.

(n) "**Processor**" means a natural or legal person that Processes Personal Data on behalf of a Controller.

(o) "**Restricted Transfer**" means the disclosure, grant of access, or other transfer of Customer Personal Data to any person located in: (i) in the context of the EU GDPR, any country or territory outside the European Economic Area ("**EEA**") that does not benefit from an adequacy decision from the European Commission (an "**EU Restricted Transfer**"); (ii) in the context of the UK GDPR, any country or territory outside the UK that does not benefit from an adequacy decision from the UK Government (a "**UK Restricted Transfer**"); and (iii) with respect to the FADP, any country or territory outside of Switzerland that does not benefit from an adequacy decision from the relevant Swiss authorities (a "**Swiss Restricted Transfer**"), in each case, which would be prohibited without a legal basis under the EU or UK GDPR or FADP (as applicable).

(p) "**SCCs**" means the standard contractual clauses approved by the European Commission pursuant to implementing Decision (EU) 2021/914.

(q) "**Services**" means those services and activities to be supplied to or carried out by or on behalf of Teraswitch for Customer pursuant to the Agreement.

(r) "**State Privacy Laws**" means, collectively, the U.S. state comprehensive data privacy laws currently in effect and applicable to Teraswitch's Processing of Customer Personal Data under the Agreement.

(s) "**Sub-Processor**" means a third party engaged by Teraswitch to Process Customer Personal Data on its behalf.

(t) "**Supervisory Authority**": (i) in the context of the EEA and the EU GDPR, shall have the meaning given to that term in the EU GDPR; (ii) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office ("**ICO**"); and (iii) in the context of Switzerland and the FADP, means the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**").

(u) "**UK Transfer Addendum**" means the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the UK Mandatory Clauses included in Part 2 thereof (the "**UK Mandatory Clauses**").

1.2 All capitalized terms not defined in this DPA shall have the meaning given to them in the Agreement.

2. **PROCESSING OF CUSTOMER PERSONAL DATA**

2.1 Details and roles. The Parties acknowledge and agree that the details of Teraswitch's Processing of Customer Personal Data (including the respective roles of the Parties relating to such Processing) are as described in Annex 1 (Data Processing Details) to the DPA.

2.2 General. Teraswitch shall not Process Customer Personal Data other than: (a) on Customer's instructions set out in the Agreement and this DPA; or (b) as required by applicable laws, provided that in such circumstances, Teraswitch shall inform Customer in advance of the relevant legal requirement if and to the extent Teraswitch is: (i) required to do so by Applicable Data Protection Laws; and (ii) permitted to do so in the circumstances. Customer instructs and authorizes Teraswitch to Process Customer Personal Data for the purposes set out in the Agreement, as further described in Annex 1 (Data Processing Details) to the DPA. The Agreement is a complete expression of such instructions, and Customer's additional instructions will be binding on Teraswitch only pursuant to a written amendment to this DPA signed by both Parties. Where required by Applicable Data Protection Laws, Teraswitch shall notify Customer if (in its reasonable opinion) an instruction from Customer violates Applicable Data Protection Laws. Teraswitch may, as part of providing the Services, anonymize or aggregate Customer Personal Data in accordance with the standards for such activity set forth in Applicable Data Protection Laws. For the avoidance of doubt, such anonymized or aggregated data, whichever the case may be, will not be subject to the requirements and restrictions set forth in this DPA. If Teraswitch anonymizes Customer Personal Data, or receives anonymized data from Customer, Teraswitch will, where required by Applicable Data Protection Laws, (i) take reasonable measures to ensure that such anonymized data cannot be associated with an individual; (ii) publicly commit to maintain and use the data in anonymized form and to not attempt to re-identify the data; and (iii) contractually obligate any recipients of the anonymized data to comply with the terms of this Section 2.2 and Applicable Data Protection Laws.

3. **TECHNICAL AND ORGANIZATIONAL MEASURES; ASSISTANCE**

3.1 Personnel. Teraswitch shall impose confidentiality obligations on all Teraswitch Personnel who Process Customer Personal Data that are not otherwise subject to professional or statutory confidentiality obligations.

3.2 Security. Teraswitch shall implement and maintain technical, administrative, physical, and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, and access, as described in Annex 3 (Security Measures) (the "**Security Measures**"). Teraswitch may modify these Security Measures from time to time to reflect its then-current security standards and practices, provided that such modifications do not materially decrease the overall security of the relevant Customer Personal Data.

3.3 Data Subject Requests. Teraswitch, taking into account the nature of the Processing of Customer Personal Data, shall provide Customer with such assistance as may be reasonably necessary and technically feasible to assist Customer in fulfilling its obligations to respond to Data Subject Requests, including requests to access, delete, and cease Processing of Customer Personal Data. If Teraswitch receives a Data Subject Request, Customer will be responsible for responding to any such request. Teraswitch shall: (a) promptly notify Customer if it receives a Data Subject Request; and (b) not respond to any Data Subject

Request, other than to advise the Data Subject to submit the request to Customer, except as required by Applicable Data Protection Laws.

3.4 DPIAs and consultations. If and to the extent expressly required by Applicable Data Protection Laws (including, where applicable, by the GDPR), in relation to the given Processing of Customer Personal Data, Teraswitch shall, taking into account the nature of the Processing and the information available to it, provide reasonable assistance to Customer with any data protection impact assessments and prior consultations with Supervisory Authorities that are required by Applicable Data Protection Laws (including, where applicable, Article 35 or Article 36 of the GDPR), in each case solely in relation to such Processing of Customer Personal Data by Teraswitch.

4. PERSONAL DATA BREACHES

4.1 Notifications. Teraswitch shall notify Customer without undue delay upon Teraswitch's confirmation of a Personal Data Breach affecting Customer Personal Data. Teraswitch shall provide Customer with information (insofar as such information is within Teraswitch's possession and knowledge and does not otherwise compromise the security of Teraswitch's information technology systems or practices or any Personal Data Processed by Teraswitch) designed to enable Customer to meet its obligations under Applicable Data Protection Laws to report the Personal Data Breach. This notification will include Teraswitch's then-current assessment of the following, to the extent available, which may be based on incomplete information: (a) the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects and Customer Personal Data records concerned; (b) the likely consequences of the Personal Data Breach; and (c) measures taken or proposed to be taken by Teraswitch to address the Personal Data Breach, including, where applicable, measures designed to mitigate its likely adverse effects. Teraswitch's notification of or response to a Personal Data Breach shall not be construed as Teraswitch's acknowledgment of any fault or liability with respect to the Personal Data Breach. Nothing in this DPA or in the SCCs shall be construed to require Teraswitch to violate, or delay compliance with, any legal obligation it may have with respect to a Personal Data Breach or other security incidents generally. As between the Parties, Customer is solely responsible for complying with applicable laws (including breach notification laws) and fulfilling any third-party notification obligations related to a Personal Data Breach.

4.2 Consultation with Teraswitch. If Customer determines that a Personal Data Breach must be notified to any Supervisory Authority, any other governmental authority, any Data Subject(s), the public, or others under Applicable Data Protection Laws or otherwise, to the extent such notice directly or indirectly refers to or identifies Teraswitch, where permitted by applicable laws, Customer agrees to: (a) notify Teraswitch in advance; and (b) in good faith, consult with Teraswitch and consider any clarifications or corrections Teraswitch may reasonably recommend or request to any such notice that: (i) relate to Teraswitch's involvement in or relevance to such Personal Data Breach; and (ii) are consistent with applicable laws.

5. SUB-PROCESSING

5.1 General authorization. Customer generally authorizes Teraswitch to appoint Sub-Processors in accordance with this Section 5. Information about Teraswitch's Sub-Processors, including their functions and locations, is as shown from time to time in the Sub-Processor list displayed from time to time at trust.teraswitch.com (the "**Sub-Processor List**"). Customer authorizes

Teraswitch's engagement of the Sub-Processors listed on the Sub-Processor List as of the Agreement effective date.

5.2 Notification. Teraswitch shall give Customer prior written notice of the appointment of any proposed Sub-Processor, including reasonable details of the Processing to be undertaken by the Sub-Processor, by updating its Sub-Processor List. If, within ten (10) business days of receipt of that notice, Customer notifies Teraswitch in writing of any objections to the proposed appointment (made in good faith based upon evidenced concerns that use of the proposed Sub-Processor would cause Customer to be in material and unavoidable breach of Applicable Data Protection Laws): (a) Teraswitch shall use reasonable efforts to make available a commercially reasonable change in the provision of the Services that avoids use of that proposed Sub-Processor; and (b) where: (i) such a change cannot be made within thirty (30) days from Teraswitch's receipt of Customer's notice; (ii) no commercially reasonable change is available; and/or (iii) Customer declines to bear the cost of the proposed change, then either Party may terminate without penalty the Processing of Customer Personal Data and/or the Agreement with respect only to those services that cannot be provided by Teraswitch without the use of the objected-to new Sub-Processor by providing written notice to the other Party. If Customer does not object to Teraswitch's appointment of a Sub-Processor during the objection period referenced in this Section 5.2, Customer shall be deemed to have approved the engagement and ongoing use of that Sub-Processor.

5.3 Teraswitch responsibilities. Teraswitch shall enter into a written agreement with each Sub-Processor containing, in substance, data protection obligations no less protective than those set out in this DPA (including the Security Measures) with respect to the protection of Customer Personal Data to the extent applicable to the nature of the Services provided by such Sub-Processor. As between the Parties, Teraswitch shall remain liable for any breach of this DPA caused by a Sub-Processor.

6. DATA TRANSFERS

6.1 Entry into SCCs. With respect to any Restricted Transfer of Customer Personal Data from Customer to Teraswitch under this DPA: (a) that is an EU Restricted Transfer, the Parties hereby enter into and agree to comply with their respective obligations set out in the SCCs; (b) that is a UK Restricted Transfer, the Parties hereby enter into and agree to comply with their respective obligations set out in the SCCs as varied by the UK Transfer Addendum in accordance with Section 6.3; and/or (c) that is a Swiss Restricted Transfer, the Parties hereby enter into and agree to comply with their respective obligations set out in the SCCs as varied in accordance with Section 6.4.

6.2 Population of SCCs. With respect to any SCCs entered into pursuant to Section 6.1, the Parties agree as follows: (a) each of the Parties is hereby deemed to have signed the SCCs at the relevant signature block in Annex I to the Appendix to the SCCs; (b) as applicable: (i) Module Two of the SCCs applies to any relevant Restricted Transfer involving Processing of Customer Personal Data and Usage Data with respect to which Customer is a Controller in its own right; and (ii) Module Three of the SCCs applies to any relevant Restricted Transfer involving Processing of Customer Personal Data with respect to which Customer is itself a Processor; (c) as and where applicable to the relevant Module of the SCCs and the Clauses thereof: (i) in Clause 7: the 'Docking Clause' is not used; (ii) in Clause 9: 'OPTION 2: GENERAL WRITTEN AUTHORIZATION' applies, and the minimum time period for advance notice of the addition or replacement of Sub-Processors shall be the advance notice period

set out in Section 5.2; (iii) in Clause 11: the optional language is not used; (iv) in Clause 13: all square brackets are removed and all text therein is retained; (v) in Clause 17: 'OPTION 1' applies, and the Parties agree that the SCCs shall be governed by the law of: (A) Ireland in relation to any EU Restricted Transfer; (B) England and Wales in relation to any UK Restricted Transfer; and (C) Switzerland in relation to any Swiss Restricted Transfer; and (vi) in Clause 18(b): the Parties agree that any dispute arising from the SCCs shall be resolved by: (A) in relation to any EU Restricted Transfer, the courts of Ireland; (B) in relation to any UK Restricted Transfer, the courts of England and Wales; and (C) in relation to any Swiss Restricted Transfer, the courts of Switzerland; and (d) with respect to the Annexes to the Appendix to the SCCs: (i) Annex I is populated with the corresponding information detailed in Annex 1 (Data Processing Details) to the DPA; and (ii) Annex II is populated with reference to the information contained in and determined by Section 3.2 of the DPA (including the Security Measures).

6.3 Population of UK Transfer Addendum. Where relevant in accordance with Section 6.1(b), the SCCs apply to any UK Restricted Transfers as varied by the UK Transfer Addendum in the following manner: (i) 'Part 1 to the UK Transfer Addendum': (A) Tables 1, 2 and 3 to the UK Transfer Addendum are deemed populated with the corresponding details set out in Annex 1 (Data Processing Details) to the DPA and Section 6.2; and (B) Table 4 to the UK Transfer Addendum is completed by the box labeled 'Data Importer' being deemed to have been checked; and (ii) 'Part 2 to the UK Transfer Addendum': the Parties agree to be bound by the UK Mandatory Clauses and that the SCCs shall apply to any UK Restricted Transfers as varied in accordance with those Mandatory Clauses.

6.4 Swiss Restricted Transfers. To the extent that any Processing of Customer Personal Data under this DPA involves a Swiss Restricted Transfer from Customer to Teraswitch, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be: (a) populated in accordance with Section 6.2; (b) varied in the following manner: (i) the FDPIC shall be the sole Supervisory Authority for Swiss Restricted Transfers exclusively subject to the FADP (including for the purposes of Annex I.C to the Appendix to the SCCs and the competent Supervisory Authority referenced therein); (ii) the terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the SCCs shall be interpreted to include the FADP with respect to Swiss Restricted Transfers; (iii) references to Regulation (EU) 2018/1725 are removed; (iv) references to the "Union", "EU" and "EU Member State" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the SCCs; (v) where Swiss Restricted Transfers are exclusively subject to the FADP, all references to the GDPR in the SCCs are to be understood to be references to the FADP; and (vi) where Swiss Restricted Transfers are subject to both the FADP and the GDPR, all references to the GDPR in the SCCs are to be understood to be references to the FADP only insofar as the Swiss Restricted Transfers are subject to the FADP; and (c) entered into by the Parties and incorporated by reference into this DPA.

6.5 Operational clarifications. In relation to any SCCs entered into pursuant to Section 6.1, the Parties agree as follows: (a) when complying with its transparency obligations under Clause 8.3 of the SCCs, Customer shall not provide or otherwise make available, and shall take all appropriate steps to protect, Teraswitch's and its licensors' trade secrets, business secrets, confidential information and/or other commercially sensitive information; (b) where applicable, for the purposes of Clause 10(a) of Module Three of the SCCs, Customer acknowledges and agrees that there are no circumstances in which it would be appropriate for Teraswitch to

notify any third party Controller of any Data Subject Request and that any such notification shall be the sole responsibility of Customer; (c) for the purposes of Clause 15.1(a) of the SCCs, except to the extent prohibited by applicable law and/or the relevant public authority, as between the Parties, Customer agrees that it shall be solely responsible for notifying relevant Data Subject(s) if and as required; (d) the terms and conditions of Section 5 apply in relation to Teraswitch's appointment and use of Sub-Processors under the SCCs; (e) any approval by Customer of Teraswitch's appointment of a Sub-Processor that is given expressly or deemed given pursuant to Section 5 constitutes Customer's documented instructions to effect disclosures and onward transfers to any relevant Sub-Processors if and as required under Clause 8.8 of the SCCs; (f) the audits described in Clauses 8.9(c) and 8.9(d) of the SCCs shall be subject to any relevant terms and conditions detailed in Section 6; (g) certification of deletion of Customer Personal Data as described in Clauses 8.5 and 16(d) of the SCCs shall be provided only upon Customer's written request; (h) in relation to any: (i) UK Restricted Transfer to which they apply, where the context permits and requires, any reference in the DPA to the SCCs, shall be read as a reference to those SCCs as varied by Section 6.3; and (ii) Swiss Restricted Transfer to which they apply, where the context permits and requires, any reference in the DPA to the SCCs, shall be read as a reference to those SCCs as varied by Section 6.4; and (i) with respect to any given Restricted Transfer, if requested of Customer by a Supervisory Authority, Data Subject, or further Controller (where applicable), on specific written request, accompanied by suitable supporting evidence of the relevant request, Teraswitch shall provide Customer with an executed version of the relevant set(s) of SCCs responsive to the request made of Customer (amended and populated in accordance with relevant provisions of this DPA with respect to the relevant Restricted Transfer) for countersignature by Customer, onward provision to the relevant requestor and/or storage to evidence Customer's compliance with Applicable Data Protection Laws.

6.6 Alternative Transfer Mechanisms. If and where Teraswitch is or becomes certified under an Alternative Transfer Mechanism, the Parties will rely on such Alternative Transfer Mechanism for all relevant Processing of Customer Personal Data covered thereby that would otherwise have involved a Restricted Transfer to Teraswitch, and the SCCs shall not apply. As and where relevant, Teraswitch shall ensure that its Processing of relevant Customer Personal Data covered by such Alternative Transfer Mechanism accords with relevant principles and requirements thereof. As and where Teraswitch is not certified under such an Alternative Transfer Mechanism, Teraswitch withdraws from any such Alternative Transfer Mechanism and/or the relevant adequacy decision for the Alternative Transfer Mechanism is invalidated, the Parties shall be deemed to have automatically entered into the relevant SCCs applicable to such previously covered Restricted Transfer in accordance with the remaining provisions of this Section 6.

7. AUDITS

7.1 Information provision and audits. Teraswitch shall make available to Customer, upon reasonable request by Customer or its designee, such information as Teraswitch (acting reasonably) considers appropriate in the circumstances to demonstrate its compliance with this DPA. Subject to Sections 7.2 to 7.4, in the event that Customer (acting reasonably) is able to provide documentary evidence that such information is not sufficient in the circumstances to demonstrate Teraswitch's compliance with this DPA, Teraswitch shall, subject to the provisions in this Section 7, allow for and contribute to audits by Customer or an auditor mandated by Customer in relation to the Processing of Customer Personal Data by Teraswitch.

7.2 Customer responsibilities. Customer shall: (a) give Teraswitch reasonable notice of any audit to be conducted under Section 7.1 (which shall in no event be less than thirty (30) days' notice, unless a shorter notice period is specifically required under Applicable Data Protection Laws relevant to the audit concerned); (b) where appropriate (as determined at Teraswitch's discretion), conduct all audits remotely via means made available by Teraswitch for that purpose; and (c) use its best efforts (and ensure that each of its mandated auditors uses its best efforts) to avoid causing any destruction, damage, injury, or disruption to Teraswitch's premises, equipment, Personnel, data, and business (including any interference with the confidentiality or security of the data of Teraswitch's other customers or the availability of Teraswitch's services to such other customers).

7.3 Audit plans. Prior to conducting any audit, Customer must submit a detailed proposed audit plan providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof as Teraswitch's Confidential Information. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Teraswitch will review the proposed audit plan and provide Customer with any feedback, concerns, or questions. Teraswitch will work cooperatively with Customer to agree on a final audit plan.

7.4 Limitations. Teraswitch need not give access to its premises for the purposes of any audit under this Section 7: (a) where a third party audit report or certification (e.g., SOC 2 Type 2 or similar audit report or certification) is provided in lieu of such access (acceptance of which for this purpose not to be unreasonably withheld, delayed, or conditioned by Customer); (b) to any individual unless they produce reasonable evidence of their identity; (c) to any auditor whom Teraswitch has not approved in advance (acting reasonably); (d) to any individual who has not entered into a nondisclosure agreement with Teraswitch on terms acceptable to Teraswitch (acting reasonably); (e) outside normal business hours at those premises; or (f) on more than one occasion in any calendar year during the term of the Agreement, except for any audits that Customer is required to carry out under Applicable Data Protection Laws or by a Supervisory Authority. Nothing in this DPA shall require Teraswitch to furnish more information about its Sub-Processors in connection with such audits than such Sub-Processors make generally available to their customers. Nothing in this Section 7 shall be construed to obligate Teraswitch to breach any duty of confidentiality.

8. RETURN AND DELETION

8.1 General. Upon expiration or earlier termination of the Agreement, Teraswitch shall return and/or delete all Customer Personal Data in Teraswitch's care, custody, or control in accordance with Customer's instructions as to the post-termination return and deletion of Customer Personal Data expressed in the Agreement. To the extent that deletion of any Customer Personal Data contained in any backups maintained by or on behalf of Teraswitch is not technically feasible within the timeframe set out in Customer's instructions, Teraswitch shall (a) securely delete such Customer Personal Data in accordance with any relevant scheduled backup deletion routines (e.g., those contained within Teraswitch's relevant business continuity and disaster recovery procedures); and (b) pending such deletion, put such Customer Personal Data beyond use other than for storage within such backups.

8.2 Permitted retention. Notwithstanding the foregoing, Teraswitch may retain Customer Personal Data where required by applicable laws or as otherwise permitted in the Agreement, provided that Teraswitch shall Process the Customer Personal Data only as necessary for such purpose(s).

9. CUSTOMER RESPONSIBILITIES

9.1 Security. Customer agrees that, without limiting Teraswitch's obligations under Section 3.2 (Security), Customer is solely responsible for its use of the Services, including (a) making appropriate use of the Services to maintain a level of security appropriate to the risk with respect to the Customer Personal Data; (b) securing the account authentication credentials, systems, and devices Customer uses to access the Services; and (c) backing up Customer Personal Data.

9.2 Customer's security assessment. Customer has determined that the Services, the Security Measures, and Teraswitch's commitments under this DPA are adequate to meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Laws, and provide a level of security appropriate to the risk with respect to Customer Personal Data.

9.3 Compliance. Customer shall ensure that: (a) there is, and will be throughout the term of the Agreement, a valid legal basis for the Processing by Teraswitch of Customer Personal Data in accordance with this DPA and the Agreement (including, any and all instructions issued by Customer from time to time with respect to such Processing) for purposes of all Applicable Data Protection Laws (including Article 6, Article 9(2), and/or Article 10 of the GDPR, where applicable); and (b) all Data Subjects have (i) been presented with all required notices and statements (including as required by Article 12-14 of the GDPR, where applicable); and (ii) provided all required consents, in each case (i) and (ii) relating to the Processing by Teraswitch of Customer Personal Data.

9.4 Restricted data. Customer shall not provide or otherwise make available to Teraswitch any data or information that contains any (a) health insurance information, Protected Health Information subject to the Health Insurance Portability and Accountability Act (HIPAA), or other information regarding an individual's health, medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (b) biological or biometric data; or (c) any payment card information subject to the Payment Card Industry Data Security Standard.

10. VARIOUS

10.1 Incorporation and application. This DPA shall be incorporated into and form part of the Agreement. This DPA: (a) applies only if and to the extent Applicable Data Protection Laws govern Teraswitch's Processing of Customer Personal Data in performance of the Services as a Processor (or similar role defined under Applicable Data Protection Laws); and (b) does not apply to Teraswitch's Processing of any Personal Data for its own business or customer relationship administration purposes, its own marketing or service analytics, its own information and systems security purposes supporting the operation of the Services, or its own legal, regulatory, or compliance purposes.

10.2 State Privacy Laws. Annex 2 (State Privacy Laws Annex) applies if and to the extent Teraswitch's Processing of Customer Personal Data is subject to the State Privacy Laws.

10.3 Costs. Except to the extent prohibited by Applicable Data Protection Laws, Customer shall compensate Teraswitch at Teraswitch's then-current professional services rates for, and reimburse any costs reasonably incurred by Teraswitch in the course of providing cooperation, information, or assistance requested by Customer pursuant to Sections 3.3

(Data Subject Requests), 3.4 (DPIAs and consultations) and 7 (Audits) of this DPA (provided that Teraswitch shall bear its own costs in the event that any audit or inspection conducted in accordance with Section 7 reveals any material noncompliance by Teraswitch with this DPA and/or Applicable Data Protection Laws), in each case, beyond providing self-service features included as part of, or in connection with, the Services.

10.4 LIABILITY. THE TOTAL AGGREGATE LIABILITY OF EITHER PARTY TOWARDS THE OTHER PARTY, HOWSOEVER ARISING, UNDER OR IN CONNECTION WITH THIS DPA AND THE SCCS (IF AND AS THEY APPLY) WILL UNDER NO CIRCUMSTANCES EXCEED ANY LIMITATIONS OR CAPS ON, AND SHALL BE SUBJECT TO ANY EXCLUSIONS OF, LIABILITY AND LOSS AGREED BY THE PARTIES IN THE AGREEMENT; PROVIDED THAT, NOTHING IN THIS SECTION 10.4 WILL AFFECT ANY PERSON'S LIABILITY TO DATA SUBJECTS UNDER THE THIRD PARTY BENEFICIARY PROVISIONS OF THE SCCS (IF AND AS THEY APPLY).

10.5 Updates. Each Party shall act in good faith to agree variations to this DPA that are reasonably necessary to address the requirements of Applicable Data Protection Laws from time to time. Without limiting the foregoing, Teraswitch may on notice vary this DPA and replace the relevant SCCs, or apply any Alternative Transfer Mechanism, so as to enable the lawful transfer of Customer Personal Data by Customer to Teraswitch under this DPA in compliance with Applicable Data Protection Laws.

10.6 Prevail. In the event of any conflict or inconsistency between: (a) this DPA and the Agreement, this DPA shall prevail; or (b) any SCCs entered into pursuant to Section 6 and this DPA and/or the Agreement, the SCCs shall prevail with respect to the Restricted Transfer to which they apply.

Annex 1

Data Processing Details

DETAILS OF PROCESSING

Categories of Data Subjects:	Any individuals whose Personal Data is comprised within Content Data, which will be as determined by Customer in its sole discretion through its use of the Services.
Categories of Personal Data:	Any Personal Data comprised within Content Data, which will be as determined by Customer in its sole discretion through its use of the Services.
Sensitive Data:	**Categories of sensitive data**. Any sensitive data comprised within Content Data, which will be as determined by Customer in its sole discretion through its use of the Services, subject to Section 9.4 of the DPA.
Frequency of Transfer:	Ongoing – as initiated by Customer in and through its use, or use on its behalf, of the Services.
Nature of the Processing:	Processing operations required in order to provide the Services in accordance with the Agreement, including collection, recording, organization, structuring, storage, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure, and/or destruction.
Purpose of the Processing:	Processing necessary to provide the Services.
Duration of Processing / Retention Period:	For the period determined in accordance with the Agreement and DPA, including Section 8 of the DPA
Transfers to Sub-Processors:	Transfers to Sub-Processors are as, and for the purposes, described from time to time in the Sub-Processor List.
Competent Supervisory Authority:	If and where applicable, having regard to Section 6 of the DPA: ● **EU Restricted Transfers**: the competent Supervisory Authority shall be determined as follows: (i) where Customer is established in an EU Member State: the competent Supervisory Authority shall be the Supervisory Authority of that EU Member State in which Customer is established; and (ii) where Customer is not established in an EU Member State, Article 3(2) of the GDPR applies and Customer has appointed an EU Representative under Article 27 of the GDPR: the competent Supervisory Authority shall be the Supervisory Authority of the EU Member State in which Customer's EU Representative relevant to the Processing

	hereunder is based (from time-to-time), which Customer shall notify to Teraswitch in writing. ● **UK Restricted Transfers**: the ICO. ● **Swiss Restricted Transfers**: the FDPIC.

Annex 2

State Privacy Laws Annex

1. For purposes of this Annex 2, the terms “business,” “business purpose,” “commercial purpose,” “Consumer,” “sell,” “share,” and “service provider” shall have the respective meanings given thereto in the State Privacy Laws, and “personal information” shall mean Customer Personal Data that constitutes personal information governed by the State Privacy Laws.

2. It is the parties’ intent that with respect to any personal information, Teraswitch is a service provider. Teraswitch (a) acknowledges that personal information is disclosed by Customer only for the limited and specified business purposes described in the Agreement and the DPA; (b) shall comply with applicable obligations under the State Privacy Laws and shall provide the same level of privacy protection to personal information as is required by the State Privacy Laws; (c) agrees that Customer has the right to take reasonable and appropriate steps to help to ensure that Teraswitch’s use of personal information is consistent with Customer’s obligations under the State Privacy Laws; (d) shall notify Customer in writing of any determination made by Teraswitch that it can no longer meet its obligations under the State Privacy Laws; and (e) agrees that Customer has the right, upon notice, including pursuant to the preceding clause, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

3. For purposes of the California Consumer Privacy Act of 2018, Teraswitch will Process personal information for the following business purposes: (i) performing the Services on behalf of Customer, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying information, providing analytic services, providing storage, or providing similar services on behalf of Customer; (ii) helping to ensure security and integrity; (iii) debugging to identify and repair errors that impair existing intended functionality; (iv) short-term, transient use; and (v) undertaking internal research for technological development and demonstration; and (vi) undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by Customer, and to improve, upgrade, or enhance such service or device.

4. Teraswitch shall not (a) sell or share any personal information; (b) retain, use, or disclose any personal information for any purpose other than for the specific purpose of providing the Services, including retaining, using, or disclosing the personal information for a commercial purpose other than the provision of the Services, or as otherwise permitted by the State Privacy Laws; (c) retain, use, or disclose the personal information outside of the direct business relationship between Teraswitch and Customer; or (d) combine personal information received pursuant to the Agreement with personal information (i) received from or on behalf of another person, or (ii) collected from Teraswitch’s own interaction with any Consumer to whom such personal information pertains, except as and to the extent necessary as a part of Teraswitch’s provision of the Services. Teraswitch hereby certifies that it understands its obligations under this Annex 2 and will comply with them.

5. To the extent permitted by the State Privacy Laws, Teraswitch may use, retain and otherwise Process personal information obtained in the course of providing the Services: (i) for internal use by Teraswitch to build or improve the quality of its services, provided that Teraswitch does not use the personal information to perform services on behalf of another person; (ii) to prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent or illegal activity; (iii) to comply with applicable laws; (iv) to comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by government authorities; (v) to cooperate with law enforcement agencies concerning conduct or activity that Teraswitch reasonably and in good faith believes may violate federal, state, or local law; and (vi) to exercise or defend legal claims.

6. The parties acknowledge that Teraswitch's retention, use, and disclosure of personal information authorized by Customer's instructions documented in the DPA are integral to Teraswitch's provision of the Services and the business relationship between the Parties.

Annex 3

Security Measures

Teraswitch maintains an information security program that is assessed by an external auditor through the Service Organization Controls 2, Type 2 Report or a similar or equivalent audit report or certification ("**Audit Report**"). Teraswitch will employ and maintain a data processing environment and internal controls that provide at least the same level of protection as evidenced by the controls described in Teraswitch's then-current Audit Report. Without limiting the foregoing, Teraswitch will, additionally (where applicable), implement the following security measures:

- **Organizational Controls**. Organizational management and dedicated staff responsible for the development, implementation and maintenance of Teraswitch's information security program.
- **Personnel Controls.** Personnel controls including background screening prior to hire where permitted by applicable law, written confidentiality obligations binding on employees and contractors, and security awareness training.
- **Data Security Controls**. Data security controls which include at a minimum logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available and industry standard encryption technologies for Customer Personal Data as and where appropriate to the data concerned.
- **Logical Access Controls**. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions.
- **Password Controls**. Password controls designed to manage and control password strength, reuse and usage.
- **Physical and Environmental Security**. Physical and environmental security of production resources relevant to the Services. Facility perimeter and entry control, surveillance, and power, cooling and fire suppression at data center locations are provided and maintained by the relevant Sub-Processor(s) (and their vendors) engaged from time to time by Teraswitch to host those resources. Teraswitch takes reasonable steps to ensure that such Sub-Processors provide appropriate assurances that evidence such physical and environmental security, including security of data center and server room facilities designed to protect information assets from unauthorized physical access and to guard against environmental hazards such as heat, fire and water damage.
- **Operational Procedures**. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, and for the secure disposal of systems and media.
- **Change Management**. Change management procedures and tracking mechanisms designed to classify, approve and record material changes to the production systems used to provide the Services.
- **Logging and Monitoring.** Logging of security-relevant events, retention of those records, and monitoring designed to identify activity indicative of a security event.
- **Incident Management**. Incident management procedures designed to allow Teraswitch to investigate, respond to, mitigate and notify of events related to technology and information assets applicable to the Services and Customer Personal Data, including a notification

procedure for disclosure without undue delay upon confirmation of a Personal Data Breach affecting Customer Personal Data consistent with this DPA.

- **Network Security**. Network security controls, including the use of firewalls, designed to protect systems from intrusion and limit the scope of any successful attack.

- **Sub-Processor and Vendor Management.** A register of third parties engaged in connection with the Services; security assessment of such third parties; and contractual obligations requiring protection of Customer Personal Data consistent with this DPA.

- **Vulnerability Assessment and Threat Protection**. Vulnerability assessment and threat protection technologies designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

- **Business Continuity.** Business resiliency, continuity and disaster recovery procedures designed to maintain service and to recover from foreseeable emergency situations or disasters affecting Teraswitch's own operations.