TENABLE MASTER AGREEMENT
DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") between Tenable and Customer (each a "Party" or together the "Parties") is incorporated into and made part of the Master Agreement (the "Agreement") between Customer and Tenable. The Parties agree that this DPA sets forth their obligations with respect to the Processing of Personal Data in connection with Customer's use of the Products. This DPA will remain in effect until, and automatically expire upon, the date on which Tenable ceases to process Personal Data. Capitalized terms used, but not defined in this DPA have the meanings given to them in the Agreement.

1. Definitions.

   a. "Authorized Affiliate" means any Customer's Affiliate which (i) is subject to Data Protection Legislation, and (ii) is authorized by Customer to use the Products pursuant to the Agreement, but has not signed its own agreement or order form with Tenable and is not a "Customer" as defined under the Agreement.

   b. "CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.,* as amended by the California Privacy Rights Act of 2020, and its implementing regulations.

   c. "Controller" means the Party that determines the purposes and means of the Processing of Personal Data. Controller shall be understood to include "Business" and analogous terms under Data Protection Legislation.

   d. "Data Protection Legislation" means any law, statute, regulation, or other binding restriction that applies to the Processing of Personal Data to which a Party to the Agreement is subject, including without limitation, the GDPR, the FADP, the UK GDPR, and the CCPA.

   e. "Data Subject" means (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 Legislation).

   f. **"**Deidentified Data**"** means data that cannot reasonably be used to infer information about, or otherwise be linked to, a Data Subject**.**

   g. "EU GDPR" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament.

   h. "EU Standard Contractual Clauses" means Sections I, II, III and IV (as applicable) in so far as they relate to Module 2 (Controller-to-Processor) and Module 3 (Processor-to-Processor) within the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council as approved by EC Commission Implementing Decision (EU) 2021/914 of 4 June 2021. Modules 2 and 3 shall apply as set forth in Section 11 and Schedule 1 of this DPA.

   i. "FADP" means the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1) and "Revised FADP" means the revised version of the FADP of 25 September 2020, which is scheduled to be effective on 1 January 2023.

   j. "GDPR" means the EU GDPR and/or the UK GDPR, as applicable.

   k. "Personal Data" means any information provided or made accessible by Customer relating to a Data Subject in association with Tenable's provision of the Products to Customer.

   l. "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Tenable or any Tenable Subprocessor on behalf of Customer.

m. "Process," "Processes," "Processed" or "Processing" means any operation or set of operations that is performed on Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, erasure, or destruction.

n. "Processor" means the Party that Processes the Personal Data on behalf of a Controller, including, as applicable, a "service provider" as that term is defined by the CCPA.

o. "Restricted Country" means: (i) where the EU GDPR applies, a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a country outside the UK which is not based on adequacy regulations pursuant to Section 17A of the UK Data Protection Act 2018; and (iii) where the FADP applies, a country outside Switzerland which has not been recognized to provide an adequate level of protection by the Federal Data Protection and Information Commissioner.

p. "Subprocessor" means any party that Processes Personal Data on behalf of a Processor.

q. "Supervisory Authority" means an independent public authority or a government agency established by a country, state, or territory that has appropriate jurisdiction over a Party regarding that Party's Processing of Personal Data.

r. "Tenable Personnel" means Tenable's employees and contractors who are engaged in Processing of Personal Data pursuant to this DPA.

s. "UK" means the United Kingdom of Great Britain and Northern Ireland.

t. "UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0, in force 21 March 2022) issued by the UK Information Commissioner 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 Mandatory Clauses.

u. "UK GDPR" means the United Kingdom General Data Protection Regulation, 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.

v. "Usage Data" means information regarding Customer's use of the Products that relates to Customer's interactions with the Product, behavior patterns, Product performance, and/or other diagnostic data.

2. Purpose. The purpose of this DPA is to document the agreement between the Parties relating to the Processing of Personal Data in accordance with the requirements of Data Protection Legislation. If any provision in this DPA conflicts with the Agreement, then this DPA shall prevail. If a provision of the EU Standard Contractual Clauses or UK Addendum conflicts with this DPA or the Agreement, the EU Standard Contractual Clauses and the UK Addendum, as applicable, shall prevail.

3. Roles Generally. The Parties agree that if Customer provides Tenable with Personal Data under the Agreement, then as between the Parties: (i) Customer is a Controller and/or Processor; and (ii) Tenable shall act as Processor and/or Subprocessor acting on behalf of and at the direction of Customer.

a. Customer. As between the Parties, Customer acknowledges that it has sole control over: (i) the process of obtaining Personal Data from Data Subjects and all necessary consents for such Personal Data; (ii) the categories of Data Subjects and Personal Data to be Processed; and (iii) the accuracy, quality, and lawfulness of the Processing of Personal Data and the means by which it was acquired. Customer expressly acknowledges that its use of the Products 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 Data Protection Legislation.

b. Tenable. Tenable shall Process the Personal Data as set forth in Schedule 2 and in accordance with the following: (i) the Agreement and any transaction documents thereunder; (ii) reasonable instruction provided by Customer to Tenable, which is otherwise consistent with the Agreement, including all instructions

provided via email; (iii) Processing initiated by Customer in its use of the Products; and (iv) as otherwise permitted or required by Data Protection Legislation. Tenable shall promptly inform Customer if, in the opinion of Tenable, an instruction from Customer violates any Data Protection Legislation or other applicable law. If Tenable is legally required to Process Personal Data in a manner not instructed by Customer, then it shall notify Customer without undue delay before such Processing occurs, unless the law requiring such Processing prohibits Tenable from providing such notification on an important ground of public interest, in which case Tenable shall notify Customer as soon as that law permits Tenable to do so.

i. Tenable shall not (a) "Sell" or "Share" Personal Data as those terms are defined under Data Protection Legislation (e.g., CCPA); (b) retain, use, disclose, or otherwise Process Personal Data in any manner outside of the direct business relationship between Tenable and Customer; or (c) combine any Personal Data with personal data that Tenable receives from or on behalf of any other third party or collects from Tenable's own interactions with Data Subjects, provided that Tenable may so combine Personal Data for a purpose permitted under Data Protection Legislation, or if directed to do so by Customer.

ii. Compliance with Data Protection Legislation. Tenable will Process Personal Data in accordance with Data Protection Legislation requirements directly applicable to Tenable's provision of the Products. Tenable shall promptly notify Customer upon becoming aware that Tenable can no longer comply with Data Protection Legislation, 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 Processing of Personal Data to the extent required of Customer under Data Protection Legislation.

4. Data Subjects.

a. Consent. As between the Parties, Customer is solely responsible for compliance with its obligations under Data Protection Legislation, in particular, for justification of any transmission of Personal Data to Tenable (including, to the extent required under Data Protection Legislation, providing any required notices and obtaining any required consents, or establishing an alternative justification for legally collecting Personal Data for Processing).

b. Third Party Requests. Unless prohibited by law, Tenable shall, without undue delay, inform Customer in writing in the event it receives: (i) any request received from an individual who is (or claims to be) a Data Subject regarding their Personal Data; (ii) any request, inquiry, investigation or communication from a Supervisory Authority; or (iii) any other requests with respect to Personal Data received from other third parties. Tenable shall not respond to these requests (except to confirm that such request relates to Customer), unless explicitly authorized by Customer or the response is legally required under Data Protection Legislation, a subpoena or similar legal document issued by a Supervisory Authority that compels disclosure by Tenable.

c. Assistance to Controller. Tenable shall provide reasonable assistance to Customer in response to Customer's written request for assistance in relation to: (i) a request, complaint, notice, or communication relating to Tenable's Processing of Customer Data received from a Data Subject whose Personal Data Tenable Processes on behalf of Customer; (ii) any investigation, request or notice from a Supervisory Authority; (iii) a privacy impact assessment conducted by Customer which is relevant to Customer's Processing of Personal Data in accordance with the Agreement or a transaction conducted thereunder (including consultation with the Supervisory Authority prior to Processing, where required); (iv) Customer's request (not to be made more than once per year unless requested by a Supervisory Authority) for Tenable to provide a written attestation that Tenable is in material compliance with this DPA; and (v) Customer's security obligations which are relevant to Customer's Processing of Personal Data in accordance with the Agreement.

5. Tenable Personnel. Tenable shall thoroughly inform all Tenable Personnel of their obligations of confidentiality under the Agreement, this DPA, and Data Protection Legislation, as well as to Process Personal Data in accordance with Customer's instructions. Tenable shall provide detailed training to all Tenable Personnel on the confidential nature of Personal Data. Such trainings shall include explanation of their duties and responsibilities. Tenable shall be responsible for entering into written non-disclosure agreements with Tenable Personnel who have obligations of confidentiality intended to survive the termination of Tenable Personnel's employment.

Access to Customer's Scan Data, if any, is limited to Tenable Personnel who require such access for the purpose of Processing Customer Data.

6. Subprocessors. Customer provides general authorization to Tenable to engage Subprocessors to enable Tenable to perform its obligations under the Agreement. Where Customer is a Processor, Tenable has Customer's general authorization (on behalf of the Controller) for the engagement of Subprocessors in accordance with Section 6 of this DPA. Tenable shall only engage Subprocessors that provide sufficient guarantees to implement measures that ensure that the Processing of Personal Data meets the requirements of Data Protection Legislation. Tenable shall enter into separate written agreements with each Subprocessor that contain obligations no less protective than those set forth in this DPA. Tenable shall be responsible for the acts and omissions of its Subprocessors connected with the Processing of Personal Data under this DPA. A current list of Tenable's Subprocessors is available at https://www.tenable.com/gdpr-alignment/third-party-data-sub-processors (or successor location). At least thirty (30) days before Tenable engages any new Subprocessor to perform processing activities on behalf of Customer, Tenable will update the applicable website and provide Customer with a mechanism to obtain notice of that update. Customer may object to the use of a new Subprocessor in writing within ten (10) days of such update on the website on reasonable grounds relating to the protection of the Personal Data. Tenable shall work with Customer in good faith to make available a commercially reasonable change to Customer's use of the Products that avoids the use of that proposed Subprocessor. Where such a change cannot be implemented within twenty (20) days from Tenable's receipt of Customer's objection ("Reassessment Period"), Customer may terminate the Agreement by providing written notice of termination. This termination right is Customer's sole and exclusive remedy to Customer's objection to Tenable's engagement of a new Subprocessor. No refund or relief from any payment obligation shall be available to Customer if Customer terminates the Agreement based on Tenable's choice of Subprocessor. Customer's use of the Products after the expiration of the Reassessment Period shall constitute Customer's acceptance of the new Subprocessor.

7. Personal Data Breach. In the event that Tenable becomes aware of a Personal Data Breach, Tenable shall (to the extent known and permitted under law), without undue delay after becoming aware of the Personal Data Breach, notify Customer. Such notice shall include details describing the Personal Data Breach, steps taken to mitigate the potential risks, and reasonable steps Tenable recommends Customer take to address the Personal Data Breach. Tenable may provide such information in phases as it becomes available. The Parties shall cooperate in good faith to help limit the effects of such Personal Data Breach and prevent a recurrence. Customer shall be solely responsible for providing notifications to the Supervisory Authority and/or any Data Subjects; provided, however, Tenable shall provide Customer with reasonable assistance and cooperation in carrying out such notifications. Tenable's notification of or response to a Personal Data Breach under this Section 7 will not be construed as an acknowledgement by Tenable of any fault or liability with respect to the Personal Data Breach.

8. Security of Processing. Tenable shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk associated with Processing. Specifically, Tenable shall maintain appropriate safeguards to protect Personal Data from unauthorized or unlawful Processing or a Personal Data Breach. Tenable's technical and organizational measures are available at https://static.tenable.com/prod_docs/tenable_slas.html. Tenable may change these measures at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purposes without diminishing the security level protecting Personal Data.

9. Record Keeping. Tenable shall maintain appropriate records of all Processing activities including, without limitation, the records required pursuant to Article 30(2) of the GDPR.

10. International Data Transfers. Tenable shall only transfer Personal Data across national borders or permit remote access to the Personal Data by Tenable Personnel or any Subprocessor in compliance with applicable Data Protection Legislation governing the cross-border transfer of Personal Data.

    a. Transfer of Personal Data outside of the European Economic Area ("EEA"). Subject to the additional terms set forth in Schedule 1, if Personal Data originating in the EEA is transferred (either directly or via onward transfer) via the Products to a Restricted Country, the Parties agree that the EU Standard Contractual Clauses shall apply to such transfer.

        i. Module 2 (Controller-to-Processor) of the EU Standard Contractual Clauses shall apply where Customer is a Controller.

ii. Module 3 (Processor-to-Processor) of the EU Standard Contractual Clauses shall apply where Customer is a Processor. Where Customer acts as a Processor pursuant to Module 3, Tenable acknowledges that Customer acts as Processor under the instructions of its Controller(s).

iii. Authorized Affiliates may also enter into the EU Standard Contractual Clauses with Tenable in accordance with this Section 10(a). In such a case, Customer enters into the EU Standard Contractual Clauses on behalf of its Authorized Affiliates.

b. Transfers of Personal Data outside of Switzerland. Subject to the additional terms set forth in Schedule 1, if Personal Data originating in Switzerland that is subject to the EU GDPR and the FADP is transferred (either directly or via onward transfer) via the Products to a Restricted Country, the Parties agree that the EU Standard Contractual Clauses shall apply to such transfer.

c. Transfer of Personal Data outside of the UK. Subject to the additional terms set forth in Schedule 1, if Tenable transfers Personal Data originating in the UK (either directly or via onward transfer) via the Products to a Restricted Country, the Parties agree that the EU Standard Contractual Clauses, as amended by the UK Addendum, shall apply to such transfer.

i. Authorized Affiliates may also enter into the EU Standard Contractual Clauses, as amended by the UK Addendum, with Tenable in accordance with this Section 10(c). In such a case, Customer enters into the EU Standard Contractual Clauses, as amended by the UK Addendum, on behalf of its Authorized Affiliates.

d. In the event (i) the EU Standard Contractual Clauses are amended, replaced, or repealed by the European Commission or under Data Protection Legislation, or (ii) the UK Addendum is amended, replaced or repealed by the UK Information Commissioner, the Parties shall work together in good faith to negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with Data Protection Legislation.

11. Audit Rights. Except to the extent required by Data Protection Legislation, Customer may audit Tenable's compliance with its obligations under this DPA up to once per year, unless otherwise required by a Supervisory Authority. Tenable will contribute to such audits by providing Customer or the Supervisory Authority with the information and assistance reasonably necessary to conduct the audit, including any relevant records of Processing activities applicable to the services provided by Tenable. To request an audit, Customer must submit a detailed proposed audit plan to Tenable at least two (2) weeks in advance of the proposed audit date. Tenable will review the proposed audit plan and provide Customer with any concerns or questions. Tenable will work cooperatively with Customer to agree on a final audit plan. Nothing in this section shall require Tenable to breach any duties of confidentiality. The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Tenable's health and safety or other relevant policies, and may not unreasonably interfere with Tenable business activities. If the requested audit scope is addressed in an SSAE 16/ISAE 3402 Type 2, SOC 1 or SOC 2, ISO, NIST or similar audit report performed by a qualified third-party auditor ("Audit Reports") within twelve (12) months of Customer's audit request and Tenable confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

12. Deidentified Data. To the extent Customer discloses or otherwise makes available Deidentified Data from Personal Data, or to the extent Tenable generates Deidentified Data from Personal Data, Tenable shall (a) implement reasonable measures to prohibit reidentification of the Data Subject to whom the Deidentified Data may pertain; (b) not attempt to reidentify the Deidentified Data, except that Tenable may attempt to reidentify the Deidentified Data solely for the purpose of determining whether its deidentification processes are compliant with Data Protection Legislation; and (c) contractually obligate any third party recipients of the Deidentified Data (e.g., Subprocessors) to comply with all of the provisions of this Section 12.

13. Data Retention Policy. Tenable shall implement and maintain an appropriate data retention policy that takes into account technical and legal requirements to ensure a retention period appropriate to the risk associated with Processing. Upon the termination of the Agreement, Tenable shall, at the Customer's written request, promptly

return to Customer or delete all Personal Data, provided that Tenable is not required to retain such Personal Data in order to comply with a legal obligation under applicable law.

14. Authorized Affiliates. The Parties agree that Customer enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Tenable 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 this DPA. All access and use of the Products 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.

    a. Communications. Customer shall remain responsible for coordinating all communication with Tenable under this DPA, and shall be entitled to transmit and receive any communication related to this DPA on behalf of its Authorized Affiliates.

    b. Exercise of Rights. Except where applicable Data Protection Legislation requires an Authorized Affiliate to exercise a right or seek a remedy under this DPA against Tenable 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 of 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.

15. Data Protection Contacts. Tenable's data protection representative can be contacted at privacy@tenable.com. Customer is responsible for providing notice to Tenable about Customer's data protection contact or officer. Both Parties are responsible for keeping the other Party informed of any changes to their respective data protection contacts.

List of Schedules

Schedule 1: Additional Terms for the Transfer of Personal Data Transfers Pursuant to the EU Standard Contractual Clauses and the UK Addendum
Schedule 2: Personal Data Processing Details; Technical and Organizational Measures

SCHEDULE 1
ADDITIONAL TERMS FOR PERSONAL DATA TRANSFERS PURSUANT TO THE EU STANDARD CONTRACTUAL CLAUSES AND THE UK ADDENDUM

EU Standard Contractual Clauses (Transfers Originating in the EEA and Switzerland)

1. By entering the Agreement, the Parties are deemed to have signed the EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

2. Docking Clause. The docking clause set forth in Clause 7 of Modules 2 and 3, as applicable, shall apply.

3. Instructions.

    a. *Module 2*: For the purposes of Clause 8.1(a), the following is deemed an instruction by the Customer to process Personal Data: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Customer in its use of the Products; and (iii) Processing to comply with other reasonable instructions provided by Customer in writing (e.g., via email) where such instructions are consistent with the terms of the Agreement.

    b. *Module 3*: For the purposes of Clause 8.1(a), the Customer acknowledges that its Controller has agreed that the following is deemed an instruction by the Controller to process Personal Data: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Customer in its use of the Products; and (iii) Processing to comply with other reasonable instructions provided by Customer in writing (e.g., via email) where such instructions are consistent with the terms of the Agreement.

4. Certification. The certification of deletion of Personal Data that is described in Clause 8.5 of Modules 2 and 3, as applicable, shall be provided by Tenable to Customer only upon Customer's written request.

5. Audits. The audits described in Clause 8.9(c) of Module 2 and Clause 8.9(d) of Module 3, as applicable, shall be in accordance with Section 11 of the DPA.

6. Subprocessors. Option 2 set forth in Clause 9 of Modules 2 and 3, as applicable, shall apply and "[Specify time period]" be replaced with "thirty (30) days." Any new engagements of Subprocessors by Tenable shall be made in accordance with Section 6 of the DPA.

7. Redress. The Parties agree that the Option set forth in Clause 11(a) of Modules 2 and 3, as applicable, shall not apply.

8. Supervision. For the purposes of Clause 13(a) of Modules 2 and 3, as applicable, the Customer as the data exporter shall be considered as established in an EU Member State.

9. Governing Law. In Clause 17 (Option 1) of Modules 2 and 3, as applicable, the governing law shall be the law of the Republic of Ireland.

10. Forum and Jurisdiction. In Clause 18(b) of Modules 2 and 3, as applicable, any dispute arising from the EU Standard Contractual Clauses shall be resolved by the courts located in Dublin, Republic of Ireland.

11. Additional Terms for Module 3.

    a. *Security of Processing*. For the purposes of Clause 8.6(c) and (d), Tenable shall provide notification of a Personal Data Breach to Customer (only) and not directly to the Controller. Where appropriate, Customer shall forward the notification to the Controller.

    b. *Documentation and Compliance*. For the purposes of Clause 8.9, if Tenable receives an enquiry directly from the Controller, it shall forward the enquiry to Customer and Customer will be responsible for addressing such enquiry.

    c. *Subprocessors*. For the purposes of Clause 9, Customer acknowledges that the Controller has delegated the decision making and approval authority for Subprocessing to Customer. Tenable has Customer's general authorization (on behalf of the Controller) for the engagement of Subprocessors in accordance with Section 6 of the DPA. Tenable shall follow the process set forth in Section 6 of the DPA to inform Customer (only) and not the Controller of any intended changes to that list.

    d. *Data Subject Rights*. For the purposes of Clause 10, Tenable shall notify Customer (only) and not the Controller about any request Tenable receives from a Data Subject. Where appropriate, Customer shall forward the notification to the Controller. Any authorization to respond to a request shall be provided to Tenable by Customer on behalf of the Controller. Tenable shall assist Customer as well as the Controller in fulfilling the relevant obligations to respond to any such request.

    e. *Redress*. For the purposes of Clause 11, Tenable shall handle complaints from a Data Subject in accordance with Section 5(b) of the DPA. Tenable shall only inform Data Subjects through individual notice in its capacity as the data importer if required by Data Protection Legislation. In such case, Tenable shall (to the extent permitted by Data Protection Legislation) inform Customer of that legal requirement before Tenable provides the individual notice.

    f. *Access by Public Authorities*. For the purposes of Clause 15, Tenable shall notify Customer (only) and not the Data Subject(s) in case of access by public authorities. Where appropriate, Customer shall notify the Controller and/or the affected Data Subject as necessary. If Tenable receives a request from a competent Supervisory Authority for the information Tenable preserves pursuant to Clauses 15.1 (a)-(c) or 15.2(b), it shall inform Customer and involve Customer in responding to the Supervisory Authority.

12. Additional Terms Applicable to Transfers of Personal Data Originating in Switzerland.

a. The term "EU Member State" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).

b. The EU Standard Contractual Clauses also protect the data of legal entities until the entry into force of the Revised FADP.

c. The Swiss Federal Data Protection and Information Commissioner shall act as the "competent supervisory authority" insofar as the relevant data transfer is governed by the FADP.

UK Addendum (Transfers Originating in the UK)

1. By entering the Agreement, the Parties are deemed to have signed the EU Standard Contractual Clauses, incorporated herein, including their Annexes, and the UK Addendum as of the Effective Date of the Agreement.

2. In Table 1 of the UK Addendum, the Parties' details are set forth in Section A, Schedule 2 of the DPA.

3. In Table 2 of the UK Addendum, information about the version of the EU Standard Contractual Clauses, modules, and selected clauses is set forth in this Schedule 1 of the DPA (section entitled "EU Standard Contractual Clauses (Transfers Originating in the EEA and Switzerland)").

4. In Table 3 of the UK Addendum:

   a. The list of Parties is set forth in Section A, Schedule 2, of the DPA.

   b. The description of the transfer is set forth in Section B, Schedule 2, of the DPA.

   c. Annex II is set forth in Schedule 2 of the DPA (section entitled "Technical and Organizational Measures").

   d. Annex III is set forth in Section B, Schedule 2, of the DPA (section entitled "Transfers to Subprocessors").

5. In Table 4 of the UK Addendum, both the Importer and the Exporter may terminate the UK Addendum in accordance with the terms of the UK Addendum.

6. For the purposes of the Mandatory Clauses of the UK Addendum, the Parties agree to comply with the terms of Part 2: Mandatory Clauses of the UK Addendum.

SCHEDULE 2
PERSONAL DATA PROCESSING DETAILS; TECHNICAL AND ORGANIZATIONAL MEASURES

Personal Data Processing Details

The following describes the Processing of Personal Data in accordance with the EU Standard Contractual Clauses, the UK Addendum, and other Data Protection Legislation, as applicable:

A. LIST OF PARTIES

Data Exporter: Customer (as set forth in the Agreement)
Contact Details: The email address(es) designated by Customer in Customer's account.
Data Exporter Role: As a Controller (Module 2) and/or Processor (Module 3), Customer uses Tenable's Products for its cybersecurity-related needs and/or the cybersecurity-related needs of its clients.

Data Importer: Tenable
Contact Details: Tenable Privacy Team, privacy@tenable.com
Data Importer Role: Tenable provides the Products to the data exporter under the Agreement, in the course of which it processes certain Personal Data as a Processor (Module 2) and/or Subprocessor (Module 3).

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects
Customer employees (past, present) including Product users and administrators
Customer consultants/contractors if provided access to the Products

Categories of Personal Data
Business contact details (e.g., name, address, e-mail address, phone number)
Employment details (e.g., company name, job title)
User ID and password for the Products
Usage Data
Depending on Customer's environment, naming conventions, and Scan Targets, Scan Data may contain limited Personal Data including, without limitation, user name/ID, location (city/state/country), asset and device IDs/types, IP address, file/drive/application names, and operating system types.

Tenable Cloud Security - If Customer uses Tenable Cloud Security, Customer solely determines the categories of Data Subjects and Personal Data that is made accessible to and temporarily Processed by Tenable. The Personal Data Processed depends on the Customer's cloud environment and may include, without limitation, financial information (e.g., credit card information, bank account number), and government identifiers (e.g., National ID/insurance number).

Sensitive Data Transferred
If Customer uses Tenable Cloud Security, Tenable may process health information (e.g., health insurance information).

Frequency of the Transfer
Transfers shall be made on a continuous basis.

Nature of the Processing
Tenable will process Personal Data as necessary to perform the services under the Agreement.

Purpose(s) of the data transfer and further Processing
Provision of the Products, customer relationship management (including to provide technical support) and business administration purposes.

Retention Periods
Tenable will retain Scan Data for a period of 180 days post termination of the License Term in the event Customer wishes to renew within this time period. Customer personnel contact information processed for business administration purposes, shall be retained for the duration of the License Term and in accordance with any applicable law.

Transfers to Subprocessors
A current list of Tenable Subprocessors (including location(s) of Processing) is available at https://www.tenable.com/gdpr-alignment/third-party-data-sub-processors. Tenable and its Subprocessors provide the services as set forth in the Agreement. Transfers to Subprocessors shall be on the same basis as set forth in the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Where Customer is the data exporter, the Supervisory Authority shall be the competent Supervisory Authority that has supervision over Customer.

Technical and Organizational Measures

In accordance with Annex II of the EU Standard Contractual Clauses, Annex II of the UK Addendum, and other Data Protection Legislation, as applicable, Tenable will maintain technical and organizational measures as set forth in Section 8 of the DPA. Tenable's technical and organizational measures are available at https://static.tenable.com/prod_docs/tenable_slas.html.