DATA PROCESSING ADDENDUM

(THIS "ADDENDUM")

1. Definitions

1.1 *Definitions; Construction.* Terms defined in any agreement between Company and TXOne Networks that incorporates this Addendum by reference (herein each an "**Agreement**") shall have the same meanings when used herein unless superseded or modified by a definition or text herein, in which event the term defined or conflicting text set forth herein shall govern and control. All defined terms shall be equally applicable to the singular, plural, and derivative forms. Certain of the defined terms set forth in this Addendum generally follow the definition in the GDPR and apply to all Personal Data covered herein; *provided, however*, when being read in the context of a specific Personal Data Protection Law, then such definition will be deemed to be the definition (if any) set forth in such specific Personal Data Protection Law and not the definition set forth in this Addendum. References herein to "**Company**" shall include its Affiliates that it permits to access and use any Products or Services under Company's Agreement. For the avoidance of doubt, "**Company**" herein shall not include any Contractor of Company and TXOne Networks has no obligations or liabilities hereunder to any Contractors.

"**Company's Configuration**" shall have the meaning set forth in the Agreement.

"Data Protection Impact Assessment" shall have the meaning if set forth in, and required by, an applicable Personal Data Protection Law.

"**Data Subject**" means an identified or identifiable natural person whose Personal Data is Processed by TXOne Networks in connection herewith and an Agreement.

"**European Data Protection Law**" means: (i) Regulation 2016/679 (General Data Protection Regulation) (the "**EU GDPR**"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); (iii) the EU GDPR as it is saved and incorporated into UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iv) the Privacy and Electronic Communications (EC Directive) Regulations 2003 as they continue to apply in the UK under section 2 of the European Union (Withdrawal) Act 2018; and (iv) any and all applicable national data protection law made under, pursuant, supplemental to or in order to give effect to (i) – (iv); in each case as may be amended or superseded from time to time.
The following terms shall have the meanings given to them in European Data Protection Law: "Controller", "Data Protection Impact Assessment", "Data Subject", "Process", "Processed", "Processing", "Processor" when referencing Personal Data subject thereto.

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

"**Global Privacy Notice**" means TXOne Networks's Global Privacy Notice published from time-to-time at https://www.txone.com/privacy-policy/ or as may be requested by Company from info.txone.com.

"**Party**" means each party to: (1) an Agreement that incorporates this Addendum; and/or (2) this Addendum. All other persons are third parties.

"**Permitted Purposes**" shall have the meaning set forth in clause 2.2.

"**Personal Data**" means one or more data elements relating to an identified or identifiable natural person that can be used to identify, directly or indirectly, such natural person that is made available or

supplied by Company to TXOne Networks pursuant to the Agreement and this Addendum forming a part thereof and any Personal Data generated or derived in relation to such Personal Data such as logs, if and only to the extent such data elements are regulated, protected, restricted, or controlled under an applicable Personal Data Protection Law(s).

"**Personal Data Protection Law**" means any country/regional (including, national, state/provincial, and local) enacted law that is applicable to a Party's provision, access to, and/or Processing of Personal Data under an Agreement that this Addendum is incorporated into and forms a part of, as may be enacted, amended, or superseded from time-to-time.

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

"**Products**" means software, cloud services (including SaaS products), fixed-scope managed services, and/or hardware-based appliances as may be provided by TXOne Networks to Company under the applicable Agreement that incorporates this Addendum.

"**Regulator**" means the independent public authority with responsibility for enforcing Personal Data Protection Laws in a relevant jurisdiction.

"**Security Incident**" shall have the meaning set forth in clause 3.3.

"**Services**" means support, maintenance, and/or unique technical services engagements other than Products to be provided by TXOne Networks to Company under the Agreement that incorporates this Addendum.

"**Sub-Processor**" means an entity engaged by TXOne Networks to perform certain services as described in clause 3.4.

"**TXOne Networks**" means the TXOne Networks group company that is the counterparty to the Agreement and this Addendum with Company,

1.2 Application of this Addendum. This Addendum is applicable to any TXOne Networks Agreement with Company that specifically incorporates this Addendum as a part thereof and applies to the extent TXOne Networks Processes any Personal Data as Processor or Sub-Processor for Company within the scope of an applicable Personal Data Protection Law in connection with providing any Products or Services to Company. The terms and conditions of this Addendum supersede anything to the contrary set forth in the Agreement and governs and controls the rights of the Parties with respect to the subject matter hereof.

1.3 Scope. This Addendum is applicable to all Personal Data that is Processed by TXOne Networks under an Agreement. In addition, this Addendum contains certain provisions that are only applicable to Personal Data that is subject to European Data Protection Laws.

2. Details of Processing

2.1 For clarity, this Addendum applies with respect to any Personal Data of which Company is the Controller or Processor within the scope of a Personal Data Protection Law and TXOne Networks is Processor or Sub- Processor for Company, as the case may be, of such Personal Data.

2.2 Company appoints and instructs TXOne Networks as its Processor or Sub-Processor to Process the Personal Data for the purpose of providing Products or Services to Company as described in the Agreement (or as otherwise agreed in writing between the Parties) (together the "**Permitted Purposes**").

2.3 Each Party shall comply with its obligations under Personal Data Protection Law in relation to its Processing of such Personal Data.

2.4 The subject matter, duration, nature and purpose of this Processing are as set out in Annex 1 of this Addendum.

3. TXOne Networks's Obligations Applicable to All Personal Data

3.1 If and to the extent TXOne Networks acts as Processor or Sub-Processor of any Personal Data for the Company, TXOne Networks shall only Process the Personal Data for the Permitted Purposes, and only in accordance with Company's documented instructions, unless it is required otherwise by applicable Personal Data Protection Law. TXOne Networks will notify Company promptly if it considers (but without being obliged to investigate the legal position), that: (i) it is required by any applicable Personal Data Protection Law to act other than in accordance with any Company instruction, provided that TXOne Networks is not prohibited by applicable law from such notification; or (ii) any of Company's instructions infringe or violate Personal Data Protection Law(s). Company agrees and confirms that the Agreement, this Addendum, and Company's Configuration (as defined in the Agreement) together constitute Company's complete and sole instructions to TXOne Networks regarding the Personal Data.

3.2 TXOne Networks shall ensure that any person it authorizes to process any Personal Data are subject to a duty of confidentiality (whether a contractual or statutory duty) regarding such Personal Data.

3.3 TXOne Networks shall implement appropriate and reasonable technical and organizational measures to protect the Personal Data from (i) accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure or access (a "**Security Incident**") to provide a level of security appropriate to the risk using standards of at least those set out in Annex 2 of this Addendum.

3.4 Company consents to TXOne Networks engaging third party Sub-Processors to Process the Personal Data for the Permitted Purposes provided that: (i) TXOne Networks maintains an up-to-date list of its Sub-Processors at trendmicro.com/subprocessors which it shall update with details of any change in Sub-Processors at least thirty (30) days' prior to any such change; (ii) TXOne Networks enters into a written agreement containing data protection obligations with any Sub-Processor it appoints that require the Sub-Processor to protect any Personal Data to at least the standard required by this Addendum; and (iii) TXOne Networks remains liable for any failure by its Sub-Processor to fulfil such Personal Data protection obligations (including any breach of this Addendum that is caused by an act, error or omission of its Sub-Processor). Within fourteen (14) days of publication to the above website, Company may object to TXOne Networks's appointment or replacement of a Sub-Processor, provided such objection includes Company's reasons therefor that are based solely on reasonable grounds relating to Personal Data protection.

3.5 In the event of the Company's timely objection in accordance with clause 3.4 above:

(a) TXOne Networks may elect to not appoint or to replace such Sub-Processor; or

(b) if TXOne Networks elects to use such Sub-Processor after Company's reasonable objection, Company may terminate the Agreement without penalty with effect from the date that such Sub-Processor change takes effect as to any affected Product or Service as stipulated by Company (it being understood and agreed that such right of termination is Company's sole and exclusive right and remedy if Company objects to any new or replacement Sub-Processor appointed by TXOne Networks and without prejudice to accrued fees or other rights under the Agreement).

3.6 To the extent legally permitted, in connection with TXOne Networks's processing of the Personal Data, TXOne Networks shall provide reasonable and timely assistance to Company (at Company's expense and subject to Company's payment of TXOne Networks's fees for such assistance at its standard professional services
rates prevailing at the time) to enable Company to respond to:

(a) any request from a Data Subject to exercise any of its rights under Personal Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and

(b) any other correspondence, enquiry or complaint received from a Data Subject, Regulator or other third party.

In the event that any such request, correspondence, enquiry or complaint is made directly to TXOne Networks, TXOne Networks shall promptly inform Company providing full details of the same to the extent legally permitted. Unless otherwise required by applicable law, TXOne Networks shall not disclose any Personal Data in response to any such request without Company's prior written direction.

3.7 TXOne Networks shall provide reasonable cooperation to Company (at Company's expense and subject to Company's payment of TXOne Networks's fees for such cooperation at its standard professional services rates prevailing at the time) in connection with any Data Protection Impact Assessment that may be required under Personal Data Protection Laws regarding Company's use of the Products and/or Services.

3.8 If it becomes aware of a confirmed Security Incident in relation to any Personal Data, TXOne Networks shall inform Company without undue delay and shall provide reasonable information and cooperation to Company so that Company can fulfil any Personal Data breach reporting obligations it may have under (and in accordance with the timescales required by) a Personal Data Protection Law. To the extent TXOne Networks or its Sub-Processor caused such Security Incident, TXOne Networks shall further take (or require its Sub-Processor to take) any reasonably necessary measures and actions to remedy or mitigate the effects of the Security Incident. TXOne Networks shall keep Company informed of all material developments in connection with such Security Incident without undue delay.

3.9 Upon termination or expiry of the Agreement, TXOne Networks shall (at Company's election) destroy or return to Company all Personal Data that is in TXOne Networks's possession or control (including any copies thereof). This requirement shall not apply to the extent that TXOne Networks is required by applicable laws to retain some or all Personal Data, or to Personal Data it has archived on back-up systems, in which event TXOne Networks shall securely isolate and protect such Personal Data from any further Processing (except to the extent required by such law) until deletion is possible.

3.10 TXOne Networks is committed to making available to Company all information necessary to demonstrate compliance with the obligations laid down in this Addendum and allow for and contribute to audits,

including inspections, conducted by Company or another auditor mandated by Company. In this regard, the Parties agree the following:

(a) Company acknowledges that the operation of TXOne Networks's data centers are regularly audited against ISO 27001 standards by independent third-party auditors, and includes 24x7 monitoring services and incident response, infrastructure management, change management, project management, automation tool development and technical consulting services for public cloud deployment in both on-premise data center and any applicable third party hosting service such as Amazon Web Services. Upon request, TXOne Networks shall supply a summary copy of its audit report(s) to Company, which shall be subject to the confidentiality provisions of the Agreement.

(b) After Company has exercised its rights under paragraph (a) above, if Company requires further information Company will have the right to, at its own cost and subject to Company's payment of TXOne Networks's fees in relation to such audit at its standard professional services rates prevailing at the time, require that TXOne Networks (or its independent third-party auditors) carry out a bespoke audit in relation to TXOne Networks's compliance with this Addendum. Upon receipt of such request, TXOne Networks will carry out (or arrange) such audit within such reasonable period as Company and TXOne Networks may agree, and will provide a copy of the audit report to Company promptly following conclusion of the audit.

4. Company's obligations

4.1 Company shall, in relation to the Personal Data:

(a) where required to do so, make notification(s) to any relevant Regulator in relation to its Processing of the Personal Data (including regarding any Security Incident notified to it by TXOne Networks) in an objective manner and in such a manner as not to intentionally or unreasonably bring TXOne Networks into disrepute or otherwise tarnish the reputation of TXOne Networks;

(b) ensure it is not subject to any prohibition or restriction which would: (i) prevent or restrict it from disclosing or transferring any Personal Data to TXOne Networks; (ii) prevent or restrict it from granting TXOne Networks access to any Personal Data; and/or (iii) prevent or restrict TXOne Networks from Processing any Personal Data, in each case as provided in clause 3 above;

(c) ensure that all fair Processing notices have been given (and/or, as applicable, consents obtained) in accordance with Personal Data Protection Law and are sufficient in scope to enable TXOne Networks to Process the Personal Data as provided in clause 3 above; and

(d) maintain technical and organizational security measures sufficient to comply at least with the obligations imposed on a Controller by Personal Data Protection Law.

4.2 Company's instructions for the Processing of Personal Data shall comply with Personal Data Protection Law. Company shall not give any instructions to TXOne Networks that may cause TXOne Networks to infringe any applicable law.

4.3 Any information or notices to be provided by TXOne Networks may be given to Company without having to be given to any of Company's Affiliates also.

5. Provisions Applicable to Specific Personal Data Protection Laws

5.1 Applicable Only to European Economic Area and the UK Personal Data

5.1.1 The following terms shall have the following meanings in this clause 5.1.

(a) "**Restricted Transfer**" means: (i) a transfer of Personal Data that is protected by the EU GDPR to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; or (ii) a transfer of Personal Data that is protected by the UK GDPR to a country outside of the United Kingdom which is not subject to an adequacy determination pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and

(b) "**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**").

5.1.2 TXOne Networks shall not transfer any Personal Data outside of the European Economic Area or the United Kingdom unless it has taken such measures as are necessary to ensure the transfer is in compliance with European Data Protection Law. Such measures may include (without limitation) transferring
Personal Data to a recipient: (i) in a country that the European Commission or competent UK authority (as applicable) has decided provides adequate protection for Personal Data (an "**adequacy finding**"); (ii) that has achieved binding corporate rules authorization in accordance with European Data Protection Law; or (iii) that has executed standard contractual clauses for transfers adopted or approved by the European Commission or the competent UK authority, as applicable.

5.1.3 The Parties agree that when the transfer of Personal Data from Company to TXOne Networks is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows (which shall be incorporated into, and form part of, this Addendum).

(a) In relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply to the extent that Company is a Controller of the Personal Data, and Module Three will apply to the extent that Company is a Processor of the Personal Data on behalf of a third party Controller;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be as set out in clause 3.4 of this Addendum;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(vii) Annex I of the Standard Contractual Clauses shall be deemed completed with the relevant information set out in the Agreement and Annex 1 to this Addendum; and

(viii) Annex II of the Standard Contractual Clauses shall be deemed completed with the information set out in Annex 2 to this Addendum.

(b) In relation to Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

(i) for so long as it is lawfully permitted to rely on standard contractual clauses for the transfer of Personal Data to processors set out in the European Commission's Decision 2010/87/EU of 5 February 2010 ("**Prior C2P SCCs**") for transfers of Personal Data from the United Kingdom, the Prior C2P SCCs shall apply between the Company (which, where Company is a processor on behalf of a third party Controller, it enters on behalf of that Controller) and TXOne Networks on the following
basis:

(A) Appendix 1 shall be completed with the relevant information set out in the Agreement and Annex 1 to this Addendum;

(B) Appendix 2 shall be completed with the relevant information set out in Annex 2 to this Addendum; and

(C) the optional illustrative indemnification clause will not apply.

(ii) Where sub-paragraph **Error! Reference source not found.Error! Reference source not found.** above does not apply, but Company and TXOne Networks are lawfully permitted to rely on the EU SCCs for transfers of Personal Data from the United Kingdom subject to completion of a "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under
s.119A(1) of the Data Protection Act 2018, then:

(A) the EU SCCs, completed as set out above in sub-paragraph 5.1.3(a) shall also apply to transfers of such Personal Data, subject to sub-clause **Error! Reference source not found.** below; and

(B) the UK Addendum shall be deemed executed between the transferring Company and TXOne Networks, and

i. the tables in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annex 3 to this Addendum; and

ii. the EU SCCs shall be deemed amended as specified by Part 2 of the UK Addendum in respect of the transfer of such Personal Data.

(iii) If neither sub-paragraph **Error! Reference source not found.Error! Reference source not found.** or **Error! Reference source not found.** (ii) applies, then Company and TXOne Networks shall cooperate in good faith to implement appropriate safeguards for transfers of such Personal Data as required or permitted by the UK GDPR without undue delay.

(c) In the event that any provision of this Addendum contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

5.1.4 With respect to Personal Data protected by the EU GDPR, where any such Personal Data is transferred outside the European Economic Area to a territory not at that time subject to an adequacy finding recognised under the EU GDPR TXOne Networks has entered into such standard contractual clauses for transfers of Personal Data from TXOne Networks to its Affiliates outside the European Economic Area, in relation to TXOne Networks's Processing of such Personal Data as set out in this Addendum and the Agreement.

5.1.5 With respect to Personal Data protected by the UK GDPR, where any such Personal Data is transferred outside the UK to a territory not at that time subject to an adequacy finding recognised under the UK GDPR, TXOne Networks has entered into such standard contractual clauses for transfers of Personal Data from TXOne Networks to its Affiliates outside the United Kingdom, in relation to TXOne Networks's Processing of such Personal Data as set out in this Addendum and the Agreement.

5.1.6 After Company has exercised its rights under clauses 3.103.10(a) and 3.103.10(b) above with respect to Personal Data protected by the UK GDPR or EU GDPR, if Company requires further information Company will have the right to, at its own cost and subject to Company's payment of TXOne Networks's fees in relation to such audit at its standard professional services rates prevailing at the time, require that TXOne Networks permit Company (or its independent third-party auditors) to carry out its own audit of TXOne Networks's compliance with this Addendum, following which TXOne Networks shall make available to Company all information, systems and staff necessary for Company (or its independent third-party auditors) to conduct such audit. If a third-party is to conduct the audit, the third-party must be mutually agreed to by Company and TXOne Networks and must execute a written confidentiality agreement with Company and TXOne Networks before conducting the audit. To request an audit, Company must submit a
detailed audit plan at least 60 days in advance of the proposed audit date to TXOne Networks describing the proposed scope, duration, and start date of the audit. TXOne Networks will review the audit plan and provide Company with any concerns or questions (for example, any request for information that could compromise TXOne Networks's security, privacy, employment or other relevant policies). Both Parties will work cooperatively in good faith to agree on a final audit plan. An audit must be conducted during normal business hours, and all reasonable measures must be taken to prevent unnecessary disruption to TXOne Networks's operations. Company will not exercise such audit right more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent Regulator; or (ii) if Company believes a further audit is necessary due to a Security Incident suffered by TXOne Networks.

5.2 **Applicable only to Switzerland Personal Data**

5.2.1 The following terms shall have the following meanings in this Clause 5.**Error! Reference source not found.**.

(a) "**Restricted Transfer**" means a transfer of Personal Data that is protected by the Swiss Federal Data Protection Act as amended from time to time ("**FDPA**") and the GDPR (where applicable) to a country outside of Switzerland which is not on the Swiss Federal Data Protection and Information Commissioner's ("**FDPIC**") list of countries that offers adequate protection ("**FDPIC List**"); and

(b) "**Standard Contractual Clauses**" means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

5.2.2 TXOne Networks shall not transfer any Personal Data outside of Switzerland to countries not on the FDPIC List, unless it has taken such measures as are necessary to ensure the transfer is in compliance with the FDPA and the GDPR (where applicable).

5.2.3 The Parties agree that when the transfer of Personal Data from Company to TXOne Networks is a Restricted Transfer it shall be subject to the Standard Contractual Clauses as follows (which shall be incorporated into, and form part of, this Addendum).

(a) In relation to Personal Data that is protected by the FDPA and GDPR (where applicable), the Standard Contractual Clauses will be adapted as follows ("**Swiss Adaptations**"):

(i) *Supervisory Authority*: Insofar as the Personal Data transmission is only subject to the FDPA, the FDPIC is the exclusive supervisory authority. If the Personal Data transfer is subject to both the Swiss DPA and the GDPR, then a parallel supervision takes place: FDPIC, insofar as the Personal Data transfer is governed by the Swiss DPA; EU authority insofar as the Personal Data transfer is governed by the GDPR (the criteria of Clause 13a for the selection of the competent authority must be observed);

(ii) *Applicable law for contractual claims under Clause 17*: Swiss law or the law of a country that allows and grants rights as a third party beneficiary for contractual claims regarding Personal Data transfers pursuant to the FDPA; law of an EU member state for those according to the GDPR (free choice for Module 4);

(iii) *Place of jurisdiction for actions between the Parties pursuant to Clause 18 b*: If the Personal Data transfer is subject to the FDPA, the place of jurisdiction shall be at TXOne Networks's domicile in Switzerland. If the Personal Data transfer is subject to the GDPR, then the court of an EU member state for actions concerning Personal Data transfers pursuant to the GDPR (free choice for Module 4) is the place of jurisdiction;

(iv) *Adjustments or additions concerning the place of jurisdiction for actions brought by Data Subjects*: The term "member state" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c);

(v) *Adjustments or additions regarding references to the GDPR*: the references to the GDPR should be understood as references to the FDPA insofar as the Personal Data transfers are subject to the FDPA; and

(vi) *Supplement until the entry into force of the revised FDPA*: the clauses of the EU SCC also protect the Personal Data of legal entities until the entry into force of the revised FDPA.

(b) In addition the Standard Contractual Clauses will apply completed as follows, unless already amended by the Swiss Adaptations:

(i) Module Two will apply to the extent that Company is a Controller of the Personal Data, and Module Three will apply to the extent that Company is a Processor of the Personal Data on behalf of a third party Controller;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be as set out in Section 3.4 of this Addendum;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by Swiss law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of at the domicile of TXOne Networksn in Switzerland;

(vii) Annex I of the Standard Contractual Clauses shall be deemed completed with the relevant information set out in the Agreement and Annex 1 to this Addendum;

(viii) Annex II of the Standard Contractual Clauses shall be deemed completed with the information set out in Annex 2 to this Addendum.

5.2.4 In the event that any provision of this Addendum contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

5.2.5 With respect to Personal Data protected by the FDPA and GDPR (where applicable), where any such Personal Data is transferred outside of Switzerland to countries not on the FDPIC List, TXOne Networks has entered into the Standard Contractual Clauses for transfers of such Personal Data from TXOne Networks to its Affiliates outside of Switzerland, in relation to TXOne Networks's Processing of such Personal Data as set out in this Addendum and the Agreement.

5.3 TXOne Networks will comply with the Personal Data Protection Laws of other jurisdictions to the extent that TXOne Networks Processes Personal Data that is subject to the Personal Data Protection Law of such other jurisdiction(s).

6. Liability

6.1 For the avoidance of doubt, in no event shall the maximum aggregate liability of TXOne Networks and all its Affiliates to Company and its Affiliates, including, without limitation, under the Agreement and (if applicable) any Standard Contractual Clauses previously entered into between TXOne Networks or any of its Affiliates, on the one hand, and Company and/or any of its Affiliates, on the other, exceed the maximum liability as defined under the terms of the Agreement.

7. Governing law and jurisdiction

7.1 This Addendum, the performance of the Parties hereunder, and all disputes arising out of or related hereto will be governed by and construed solely in accordance with the governing law provision of the Agreement, but giving due regard to any applicable Personal Data Protection Laws. The Parties irrevocably consent and agree to the sole and exclusive *in personam* jurisdiction of the courts (or arbitral tribunal as the case may be) as set forth in the Agreement with respect to any dispute that cannot be resolved by the Parties and all proceedings with respect thereto shall be litigated and determined solely and exclusively in such courts. Each of the Parties represents and agrees that such *in personam* jurisdiction is reasonable and fair and hereby waives any objection which it may now or hereafter have based on improper venue or forum non conveniens in such courts.

Annex 1:

Data Processing Description

This Annex I forms part of the Addendum and describes the processing that the processor will perform on behalf of the controller.

A. List of Parties

Controller / Data exporter:

Name:	The name of Company as set out in the Agreement and/or the Licence Instrument.
Address:	The address of Company as set out in the Agreement and/or the Licence Instrument.
Contact person's name, position and contact details:	The contact person (and details thereof) for the signatory of Company as set out in the Agreement or as provided separately by the Company to TXOne Networks.
Activities relevant to the data transferred under these Clauses:	TXOne Networks' provision of Products and/or Services to Company under the Agreement, to the extent this involves TXOne Networks Processing Personal Data on behalf of Company.
Signature and date:	As per the Agreement or as otherwise agreed between the Controller and the Data Importer/ Processor.
Role (controller/processor):	Company will be acting as controller and/or processor of Personal Data.

Processor / Data importer:

Name:	The name of TXOne Networks as set out in the Agreement and/or Licence Instrument.
Address:	The address ofT XOne Networks as set out in the Agreement or as separately provided to Company by TXOne Networks.
Activities relevant to the data transferred under these Clauses:	TXOne Networks offers a variety of data security products and services, Including anti-virus, anti-malware and other software and cloud products. TXOne Networks' provision of Products and/or Services to Company under the Agreement, to the extent this involves TXOne Networks Processing Personal Data on behalf of Company.
Signature and date:	As per the Agreement or as otherwise agreed between the Data Importer/ Processor and the Controller.
Role (controller/processor):	Processor.

B. Description of transfer

Purpose of the data transfer and further processing / Subject matter of Processing and processing operations	TXOne Networks offers a variety of data security products and services, including anti-virus, anti-malware and other software and cloud products. TXOne Networks's provision of Products and/or Services to Company under the Agreement, to the extent this involves TXOne Networks Processing Personal Data on behalf of Company.
Duration of processing	The term of the Agreement (plus any applicable exit period).
Nature of the Processing	The purpose of the Processing is TXOne Networks' provision of Products and/or Services under the Agreement. The nature of the Processing may include (but is not limited to) collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Categories of Personal Data transferred	Any Personal Data that Company decides to protect with TXOne Networks Products and Services. The type of Personal Data that Company chooses to provide or make available to TXOne Networks in the course of its use of TXOne Networks' Products and/or Services under the Agreement, which may include (but is not limited to) IP addresses, URL strings, DNS data, email senders and recipients, contents of emails and attachments to emails, network telemetry data, files and various other unstructured or structured information (including information or data associated with any of the foregoing), which could include Personal Data.
Sensitive Data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	The Personal Data that may be Processed would not normally concern any special categories of Personal Data and Company is advised against providing TXOne Networks with special categories of Personal Data or Personal Data relating to criminal convictions or offences.
Categories of Data Subjects whose personal data is transferred	Those Data Subjects whose Personal Data is provided or made available by Company to TXOne Networks in the course of its use of TXOne Networks' Products and/or Services under the Agreement. Data Subjects may include employees or customers of Company, at its sole discretion and control.
Frequency of the transfer:	Ongoing for the duration of TXOne Networks' provision of the Products and/or Services.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Personal Data will be retained in accordance with TXOne Networks' guidelines regarding the retention, storage, handling and disposal of records and information.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Where TXOne Networks engages sub-processors it will do so in compliance with the terms of the applicable Standard Contractual Clauses. The subject matter, nature and duration of the processing activities carried

	out by any sub-processor will not exceed the subject matter, nature and duration of the processing activities as described in this Addendum.

C. Competent supervisory authority

The competent supervisory authorities are:

- to the extent the Personal Data is protected by the EU GDPR, the supervisory authority of Ireland;
- to the extent the Personal Data is protected by the UK GDPR, the Information Commissioner; and
- insofar as the Swiss FDPA applies to the data transfers at issue, the Federal Data Protection and Information Commissioner (FDPIC).

Annex 2:

TXOne Networks Minimum Security Measures

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE PERSONAL DATA

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

The measures described below (or similarly strong measures) are, to the greatest extent possible, imposed contractually as minimum security measures on any third party service providers used to process Personal Data.

Measures of pseudonymisation and encryption of Personal Data	Deployment of end-point security solution including encryption and pseudonymization, along with high fidelity machine learning, behavioural analysis, exploit protection and advanced protection to against ransomware variants, file reputation, variant protection, browser exploit protection, web reputation (etc.) for threat and malware protection. Implementing appropriate controls to protect confidential and sensitive information from unauthorized disclosure and modification. Encryption must be applied to all information stored or transmitted as appropriate for the information classification and identified risks. Encryption key management is in place to support the use of cryptographic techniques. Encryption must be used for transmitting sensitive information where practicable. Full disk software encryption is enabled on the workstation operating system drives. Wireless access to the IT system is protected by encryption mechanisms. Pseudonymization measures include use of: • Quasi-identifier • Attribute suppression, particularly for sensitive Personal Data Encryption measures include: • HTTPS (TLS 1.2+) encryption for Personal Data transmission from Products

	to TXOne Networks backend, using industry standard algorithms and certificates. • Encryption of Personal Data at rest using the industry standard AES-256 algorithm with key rotations.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	A secure internal web portal is utilised to authorize employees' access to the relevant Personal Data, including that hosted by external service providers. This includes the following measures:
	
	<u>Confidentiality</u>
	• Carrying out information classification to classify specific assets based on the relative sensitivity of the information they contain and providing guidelines for the treatment, disclosure and use of classified information.
	• Use of Virtual Private Network (VPN).
	• Secure transmission of credentials using TLS 1.2 (or greater).
	• Passwords require a defined minimum complexity. Initial passwords must be changed after the first login. Passwords must be changed at least on a quarterly basis and must be changed immediately if compromise is suspected.
	• There are internal guidelines for the handling of passwords.
	• Employees are subject to a non-disclosure agreement and all employees undergo a security awareness training course upon hire and on a yearly basis.
	• Access control:
	  • Maintaining access controls and policies to manage what access is allowed to each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Access to information assets is limited to TXOne Networks employees and TXOne Networks requires that this is used for business purposes only. Access to information assets may be granted to other individuals and entities upon explicit permission from TXOne Networks management.
	  • Users are provided with access to the network, services, applications and operating systems that have been

	specifically authorized by TXOne Networks management and on a 'need to know' basis. • Regular review of all access granted to users. Accounts are deleted when the user no longer requires access to the specific processing system. • Implementing suitable measures to ensure that Personal Data collected for different purposes can be processed separately. Personal Data is processed in production network, separated from the internal network. <u>Integrity</u> • Use of firewalls to implement network access control; network Intrusion Detection System / Intrusion Prevention System (IDS/IPS) to protect against known, unknown, and undisclosed vulnerabilities; the secure web gateway for application control with zero-day exploit detection, advanced anti-malware scanning, real-time web reputation, and flexible URL filtering to provide superior internet threat protection. • Secure network interconnections ensured by firewalls etc. • Logging of transmissions of Personal Data from the IT system that stores or processes Personal Data. • Logging authentication and monitored logical system access and Personal Data access including, but not limited to, access, modification, entry and deletion of data. • Documentation of Personal Data entry rights and logging security related entries. • No possibility of deletion or modification of log files content by users. Access to the log files is logged in addition to monitoring for detecting unusual activity. • Implementing suitable measures to ensure that Personal Data are protected from accidental destruction or loss. Maintaining corrective action and incident response plans to respond to potential security threats. <u>Availability</u>

	• Information and software of all TXOne Networks critical systems is backed-up and tested regularly, to ensure and maintain the integrity and availability of information and associated assets. Personal Data is backed up to multiple durable Personal Data stores and replicated across multiple availability zones. • Protection of stored backup media. • Establishment of business continuity plans to protect critical business processes and the associated assets from the effects of major interruption, failure or disasters. • Implementation of incident response and management processes, which include internal escalation requirements. If a security incident is discovered, the incident is prioritized based on severity. A dedicated team of technical experts is assigned to investigate, advise on containment procedures, perform forensics, and manage communication. Following an incident, the team examines the root cause, and revises the response plan accordingly.
Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident	• Upon the creation of any new service at TXOne Networks, a team consisting of business and technical stakeholders is put together to create a business continuity plan containing backup, recovery and testing plans. These plans are approved by senior management and are tested at regular intervals. • Continuity Planning and Disaster Recovery Plans including: o Disaster recovery processes to restore Personal Data and processes o Recovery Time Objective (RTO) o Recovery Point Objective (RPO) o Maximum Tolerable Downtime (MTD) o Capacity management measures to monitor resource consumption of systems as well as planning of future resource requirements. • Procedures for handling and reporting incidents (incident management) including the detection and reaction to possible security incidents. • Backups of Personal Data with near-real time replication. All backups are kept

	redundant and in encrypted form (AES-256). • See also further information provided under "*Measures for ensuring ongoing confidentiality…"* above.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	• Establishment of a security organization, which has an objective to define security policies and rules for TXOne Networks operations and monitor security effectiveness. • Information and security policy adherence and control effectiveness at TXOne Networks is regularly checked through security audits and reviews by an independent party e.g. penetration tests. TXOne Networks SaaS services are scanned with leading vulnerability scanning tools. When a vulnerability is found the account owners and the InfoSec team are notified automatically. • Where third party service providers are used to process Personal Data, they are contractually required to implement processes for regular testing, assessment and evaluation of security • Information is backed-up and tested regularly.
Measures for user identification and authorisation	• See information on access control under '*Measures for ensuring ongoing confidentiality…'* above. • Segregation of access control roles (e.g. access request, access authorization, access administration) is clearly defined and documented. • Logging of transmissions of Personal Data from IT system that stores or processes Personal Data. • Logging authentication and monitored system access. • All password activities are controlled through a formal process and TXOne Networks requires that appropriate care be taken in allocation, distribution, reset and use of the passwords. • Remote access to TXOne Networks' infrastructure is strictly controlled and monitored. All authentication methods used adhere to industry best practices/standards such as certificate-based and/or multi-factor authentication.

	Where appropriate, Single Sign-On (SSO) leveraging the corporate directory is used.
Measures for the protection of Personal Data during transmission	• Sensitive information must be transported through secure or controlled means. • Secure network interconnections ensured by VPN, MFA, firewalls etc. • Remote access to the network via VPN tunnel and end-to-end encryption. • HTTPS encryption for data in transit (using TLS 1.2 or greater), using industry standard algorithms and certificates. • Where third party service providers are used to process Personal Data, they are contractually required to implement access controls and other measures to protect access to their networks.
Measures for the protection of Personal Data during storage	• Implementation of suitable measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the Personal Data media, including encryption and the use of firewalls or functionally equivalent technology to protect Personal Data. • Use of email security gateway to protect attack from email, detect the malicious URL and attachment in the email, block spam, phishing, and target attack. • Processes for the proper handling, storage and disposal of documents, computer media and systems documentation have been implemented. • All media containing sensitive or classified information is stored in a secure environment and in accordance with the manufacturer's specifications. • System documentation is stored securely. • System inputs are recorded via log files. • See information on access control under '*Measures for ensuring ongoing confidentiality…'* above.
Measures for ensuring physical security of locations at which Personal Data are processed	• TXOne Networks accords a level of protection from physical security threats and environmental hazards commensurate with the associated risks for business information and information processing facilities. • Business information and information processing facilities supporting critical or

	sensitive business activities are housed in secure areas with appropriate entry controls. All access to TXOne Networks offices and networks is strictly controlled and limited to authorized or accompanied users only. Further approval is required before entry is granted into sensitive areas. • Use of CCTV to deter, detect and analyse physical access intrusions. • All physical access by employees and contractors to TXOne Networks facilities where physical components are housed is logged and routinely audited. • Where third party service providers are used to process Personal Data, they are contractually required to implement physical security measures to protect physical access to locations at which Personal Data are processed. • See further "Measures for the protection of Personal Data during storage".
Measures for ensuring events logging	Implementation of suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data have been input into data Processing systems or removed. Maintaining audit logs of security events, and specifying minimum levels of information to be logged. Event logs are implemented and stored using management services. Implementation of suitable measures to monitor system administrators and to ensure that they act in accordance with instructions received. Logs are kept for an appropriate amount of time. Security logs are reviewed for all systems regularly by the Service Operations teams. Security event logs are also integrated with internal communication and alerting tools for real time oversight and event triage. If a security incident is suspected, it is immediately reported to the TXOne Networks InfoSec team, where a formal incident response plan is executed. In addition, InfoSec monitors TXOne Networks services environment logs. 7x24 security operation team uses Central Security Event and Information Management

	(SIEM) system to collect logs (including the logs from system, endpoint security products and network security products), and customized rules to correlate the logs to perform real-time monitor, analysis and response the security incident.
Measures for ensuring system configuration, including default configuration	• See information on access control under '*Measures for ensuring ongoing confidentiality…'* above. • Certain configuration standards are required, including that all network components and services must be configured conforming to defined TXOne Networks configuration standards. • Configuration Planning and Management. • Configuration Change Management. • Configuration Verification and Audits (changes are done through pull requests with reviews and approvals).
Measures for internal IT and IT security governance and management	Internal IT and IT security governance policies and procedures, designed to (a) satisfy security objectives, (b) identify reasonably foreseeable and internal risks to security, and (c) minimize security risks. An established "security management procedure" ensures information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken, and information security incidents are managed in a consistent and effective approach. A security organization has been established, which comprises members from top management. Security roles and responsibilities of members of the security organization and users are defined and documented in accordance with the information security policy. _ Assignment of roles and responsibilities for managing information, including an Information Manager for each function and segment. A dedicated Information Security (InfoSec) department. The InfoSec team works closely with the service operation teams and others on various aspects of security controls and training. Employees and contractors must pass security

	awareness training upon hire and regularly update knowledge. If security measures are adopted through external entities, obtaining a written description of the activities performed to help ensure compliance with security policies.
Measures for ensuring Personal Data minimisation	• The extent of Personal Data transmitted depends on how Company has configured its products, services, networks, and/or systems. • Any Personal Data received from or relating to employees or customers is deleted or pseudonymized as soon as possible. • Pseudonymization measures, see above. • See also below under 'Measures for ensuring limited Personal Data retention'. • In general, TXOne Networks only collects the minimum data required for the purpose it is seeking to achieve.
Measures for ensuring Personal Data quality	• Measures to avoid unnecessary data duplication. • Quality assurance measures. Yearly review of the inventory of major information assets to ensure its accuracy. Regularly backing up and testing information and software of all TXOne Networks critical systems to ensure and

	maintain the integrity and availability of information and associated assets.
Measures for ensuring limited Personal Data retention	• Guidelines regarding the retention, storage, handling and disposal of records and information. • Established retention schedule identifying essential record types and the period of time for which they must be retained. • Following termination, Company's Personal Data of which TXOne Networks is a Processor will be deleted in accordance with the Data Processing Addendum.
Measures for ensuring accountability	• Top TXOne Networks management is Involved in the security organization. • Responsibility is assigned to ensure end-user privacy throughout the product lifecycle and through applicable business processes. TXOne Networks management's responsibility for the TXOne Networks' information security includes: o setting information security objectives; o endorsing security strategy and direction; o endorsing information security programs, policies and processes; o ensuring appropriate level of resources available to the program; o supporting information security policy formulation, enforcement, maintenance including reviews and changes. • Personal Data privacy impact assessments are performed in accordance with applicable Personal Data Protection Law.
Measures for allowing Personal Data portability and ensuring erasure	• Certain Companies are able to login to retrieve certain Personal Data • Open formats (CSV and JSON) offered Company can export Personal Data. • Internal procedure for handling data deletion requests.

Annex 3

UK Addendum – Part 1: Tables

Table 1: Parties

Start date	The Effective Date			
The Parties	**Exporter (who sends the Restricted Transfer)**		**Importer (who receives the Restricted Transfer)**	
Parties' details	**Full legal name:**	The name of Company as set out in the Agreement and/ or Licence Instrument as provided by the Company.	**Full legal name:**	The name of TXOne Networks as set out in the Agreement and/ or Licence Instrument as provided by the TXOne Networks.
	Trading name (if different):	The trading name of Company as set out in the Agreement and/ or Licence Instrument as provided by the Company.	**Trading name (if different):**	N/A
	Main address (if a company registered address):	The address of Company as set out in the Agreement and/ or Licence Instrument as provided by the Company.	**Main address (if a company registered address):**	The address of TXOne Networks as set out in the Agreement and/ or Licence Instrument as provided by the TXOne Networks.
	Official registration number (if any) (company number or similar identifier):	The company number of Company as set out in the Agreement and/ or Licence Instrument as provided by the Company.	**Official registration number (if any) (company number or similar identifier):**	The company number of TXOne Networks as set out in the Agreement and/ or Licence Instrument as provided by the TXOne Networks.
Key Contact	The contact person (and details thereof) for the signatory of Company as set out in the Agreement or as separately provided by the Company.		The contact person (and details thereof) for the signatory of TXOne Networks as set out in the Agreement or as separately provided by the TXOne Networks.	
Signature	As per the Agreement or as otherwise agreed between the Exporter and the Data Importer.		As per the Agreement or as otherwise agreed between the Importer and the Data Exporter.	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	**Module in operation**	**Clause 7 (Docking clause)**	**Clause 11 (Option)**	**Clause 9a (Prior Authorisation or General Authorisation)**	**Clause 9a (Time period)**	**Is personal data received from the Importer combined with personal data collected by the Exporter?**

As selected in paragraph 5.1.3(a) of this Addendum.	Yes

Table 3: Appendix Information

The Appendix Information shall be deemed completed as set out in paragraph 5.1.3(a)(vii) and 5.1.3(a)(viii) of this Addendum.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: • Exporter • Importer