DATA PROCESSING TERMS FOR SUPPLIERS

If these Data Processing Terms ("Data Processing Terms") are expressly incorporated by reference into an Agreement between Sophos and Supplier, these Data Processing Terms form part of the Agreement between Supplier and Sophos where the supply of the Services involves the Processing of Sophos Personal Data.

Capitalized terms used in these Data Processing Terms are defined as set forth in Section 1 below.

BACKGROUND:

(A) Sophos Processes Personal Data in connection with their business activities.

(B) Sophos wishes to receive and Supplier wishes to provide the Services under the Agreement.

(C) Pursuant to its provision of the Services under the Agreement, Supplier may Process Sophos Personal Data.

(D) The parties wish to set forth their respective obligations and requirements pursuant to applicable Data Protection Laws and Regulations and the Processing of Sophos Personal Data pursuant to the Services and the Agreement.

(E) As such, the parties agree be bound by these Data Processing Terms, which shall apply to the Processing of Sophos Personal Data.

1. DEFINITIONS

1.1. In these Data Processing Terms, the following words and phrases shall have the following meanings:

"**Agreement**" means, collectively, the written agreement(s), including and exhibits, addenda and amendments thereto, pursuant to which Supplier provides certain Services to Sophos;

"**Affiliate**" means a company that, directly or indirectly, controls, is controlled by or is under common control with the subject entity;

"**Control**," for the purposes of this definition, means direct or indirect ownership or control of more than fifty percent (50%) of the voting interests of the subject entity;

"**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;

"**CCPA**" means the California Consumer Privacy Act as amended by the California Privacy Rights Act of 2020), codified at Cal. Civ. Code §§ 1798.100 - 1798.199.100 and the California Consumer Privacy Act Regulations issued thereto, Cal. Code Regs. tit. 11, div. 6, ch. 1, each as amended;

"**Customers**" means customers of Sophos;

"**Data Breach**" means any actual or reasonably suspected, theft or accidental or unauthorised access, use, disclosure, tampering, alteration, destruction, loss or other Processing of Sophos Personal Data;

"**Data Protection Laws and Regulations**" means all applicable laws and regulations, including where applicable laws in the EEA, the European Union, the United Kingdom, Switzerland and the United States (including, but not limited to, the CCPA) and its respective states, and equivalent

data protection laws and regulations applicable to the Processing of Personal Data under the Agreement including applicable modifications to such laws and regulations;

"**Data Subject**" means the individual to whom the Sophos Personal Data relates;

"**Data Subject Request**" means any request from a Data Subject regarding the Sophos Personal Data, including requests by Data Subjects to exercise their access, deletion, correction and other rights under the Data Protection Laws and Regulations.

"**EEA**" means the European Economic Area, including the member states of the European Union;

"**GDPR**" means the General Data Protection Regulation (EU) 2016/679;

"**Personal Data**" means any information that identifies, could be used to identify or is otherwise linked or reasonably linkable with a particular individual or household, as well as any information defined as "personal data," "personal information" or equivalent term under applicable Data Protection Laws and Regulations;

"**Personnel**" means the officers, directors, contractors, employees and other personnel of the Supplier;

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

"**Processor**" means a person or entity that Processes Personal Data on behalf and under the instructions of the Controller, including any entity acting as a "service provider" pursuant to the CCPA;

"**Restricted Transfer**" means a transfer of Sophos Personal Data by or to Supplier or a Sub-processor, including an onward transfer of Sophos Personal Data between two establishments of the Supplier or a Sub-processor, in each case where such transfer would be prohibited by applicable Data Protection Laws and Regulations in the absence of the SCCs and the UK Addendum as applicable, including any transfer of Sophos Personal Data from the EEA, United Kingdom or Switzerland to a country in respect of which a valid adequacy decision has not been issued by the European Commission or the competent Supervisory Authority, as applicable;

"**SCCs**" means 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 approved by the European Commission implementing decision (EU) 2021/914 of 4 June 2021;

"**Services**" means the services provided by the Supplier to Sophos under the terms of the Agreement;

"**Sophos**" means the entity within the Sophos group of companies that is the Sophos contracting party to the Agreement, acting for itself and for and on behalf of its Affiliates and Customers;

"**Sophos Personal Data**" means any and all Personal Data Processed pursuant to the provision of the Services and the performance of Supplier's obligations under the Agreement.

"**SOW**" means a statement of work entered into between Sophos and Supplier in relation to the Agreement;

"**Sub-processor**" means any person or entity (excluding employees of the appointing entity) appointed by or on behalf of Sophos that Processes Sophos Personal Data;

"**Supervisory Authority**" means the competent regulatory authority with regard to applicable Data Protection Laws and Regulations, including where applicable a supervisory authority as defined under the GDPR;

"**Supplier**" means the provider of the Services as set out in the Agreement;

"**UK Addendum**" means the International Data Transfer Addendum to the EU Commission SCCs, issued by the United Kingdom Information Commissioner's Office, as amended or replaced from time to time by a competent Supervisory Authority under the relevant data protection laws of the UK.

1.2. Capitalized terms used but not otherwise defined in these Data Processing Terms will have the meaning otherwise set forth in the Agreement.

2. ROLES AND PURPOSE

2.1. Parties agree that Sophos is either the Controller or Processor and Supplier is a Processor in relation to the Sophos Personal Data. Where Sophos is a Processor, it shall at all times have the authority to instruct Supplier as set forth hereunder.

2.2. The Parties will comply with their respective obligations under applicable Data Protection Laws and Regulations.

3. **PROCESSING**

3.1. **Exhibit 1** hereto sets forth a description of the Processing of the Sophos Personal Data hereunder, including the nature and purpose of the Processing, the categories of Personal Data, and the categories of Data Subjects. The parties may agree in writing to amended or additional descriptions of Processing.

3.2. Sophos instructs Supplier to Process Sophos Persona Data as reasonably necessary to the provision of the Services and the performance of the Agreement, including these Data Protection Terms.

3.3. Supplier will at all times Process Sophos Personal Data only accordance with Sophos' written instructions and in compliance with the terms of the Agreement and these Data Protection Terms, except to the extent Supplier is otherwise required to Process Sophos Personal Data pursuant to laws applicable to Supplier, in which case Supplier will inform Sophos of this requirement before the Processing unless prohibited from doing so by applicable law.

3.4. Supplier will notify Sophos immediately in writing if: (i) in Supplier's opinion, any Sophos Processing instructions infringe the Data Protection Laws and Regulations; or (ii) Supplier believes that it or a Sub-processor is or will be unable to comply with these Data Processing Terms or applicable Data Protection Laws and Regulations. Supplier will provide reasonable support and cooperation, as requested, to enable Sophos to take reasonable and appropriate steps to stop and remediate any unauthorized Processing of Sophos Personal Data.

3.5. Supplier will not:

3.5.1. Retain, use, or disclose Sophos Personal Data for any purposes other than the business purpose of performing the Services (in support of Sophos's business purposes) specified in the Agreement;

3.5.2. Process Sophos Personal Data outside of the direct business relationship between Sophos and Supplier or for Supplier's own commercial purposes;

3.5.3. Sell (as defined by CCPA) or otherwise disclose, disseminate, communicate or make available any Sophos Personal Data to any third party for monetary or other valuable consideration;

3.5.4. Share (as defined by the CCPA) any Sophos Personal Data or otherwise disclose, disseminate, communicate or make available Sophos Personal Data for cross contextual behavioural advertising;

3.5.5. Combine Sophos Personal Data with Personal Data that Supplier receives from or on behalf of another entity or collects from its own interactions with an individual; or

3.5.6. Retain or process any Sophos Personal Data for longer than is necessary to perform Supplier's obligations under the Agreement and in accordance with Section 8 hereto.

3.6. Supplier certifies it understands and will comply with the obligations and restrictions set forth in Section 3.5.

3.7. Notwithstanding Section 3.5, Supplier may engage Sub-processors provided it does so in compliance with Sections 7 and 9 hereto.

4. COOPERATION AND SUPPORT

4.1. If Supplier receives any request from a third party, including any Data Subject Request, related the Sophos Personal Data it will promptly notify Sophos and will not respond to such request, except on the documented instructions of Sophos or as required by applicable laws.

4.2. Taking into account the nature of the Processing of Sophos Personal Data, Supplier will provide reasonable assistance as necessary to: (i) assist Sophos in responding to Data Subject Requests, including where possible by implementing appropriate technical and organizational measures; (ii) enable Sophos to conduct data protection impact assessments and other privacy and data protection assessments; and (iii) notify, consult or cooperate with a Supervisory Authority as required under applicable Data Protection Laws and Regulations.

4.3. Supplier will provide Sophos with all information necessary to demonstrate Supplier's and Sub-processor's compliance with the terms of these Data Protection Terms and applicable Data Protection Laws and Regulations, including by: (i) providing complete, accurate and timely responses to reasonable data protection and security questionnaires submitted by Sophos; and (ii) allowing for and contributing to audits and inspections of Supplier's premises, resources, policies and procedures that are relevant to the provision of the Services and Processing of Sophos Personal Data, subject to the following:

4.3.1. Audits and inspections may be conducted by Sophos or its third-party auditors or agents during normal business hours and upon reasonable prior notice to Supplier; and

4.3.2. Audits and inspections shall be conducted at the cost and reasonable expense of Sophos and limited to once per calendar year, except to the extent conducted in response to a Data Breach or at the request of a Supervisory Authority.

5. BREACH NOTIFICATION

5.1. Upon discovery of a Data Breach, Supplier will notify dataprotection@sophos.com and security@sophos.com without undue delay and in any case no later than forty-eight (48) hours after the initial discovery of such Data Breach.

5.2. Supplier shall promptly provide all information and assistance that Sophos reasonably requests in the investigation, mitigation, notification, and remediation of such Data Breach. Without limiting the foregoing, the information provided by Supplier shall include sufficient information to allow Sophos to meet any obligations to notify a Supervisory Authority, Data Subjects or other third party of the Data Breach under the Data Protection Laws and Regulations, including without limitation:

5.2.1. The nature of the Data Breach, including the categories and approximate numbers of Data Subjects and Personal Data records concerned;

5.2.2. Any investigations into such Data Breach;

5.2.3. The likely consequences of the Data Breach; and

5.2.4. Any measures taken, or that Supplier recommends, to address the Data Breach, including to mitigate its possible adverse effects and prevent the re-occurrence of the Data Breach or a similar breach.

5.3. Supplier shall not, unless required by law or instructed to do so in writing by Sophos, notify any Data Subjects, third parties, or Supervisory authorities of a Data Breach. In addition, Supplier will take all steps required under applicable law and otherwise reasonably requested by Sophos or necessary to respond to and mitigate the impact of a Data Breach, including, but not limited to, reimbursing Sophos and holding it harmless for all reasonable costs related to notifications and providing credit reporting and/or monitoring services for impacted Data Subjects.

6. SECURITY AND CONFIDENTIALITY

6.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the associated risks, Supplier will implement and maintain reasonable technical, organizational and physical security measures to protect Sophos Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, access, theft, alteration or disclosure, which are appropriate to the risks, including the harm which might result from any unauthorised Processing of the Sophos Personal Data, including any unlawful or accidental loss, destruction, damage, access or theft. As a minimum, such measures shall include technical, organizational and physical security measures that meet: (i) the requirements of the Data Protection Laws and Regulations; and (ii) the requirements of these Data Processing Terms, including **Exhibit 2**.

6.2. Supplier will take reasonable steps to ensure the reliability and competence of Supplier personnel who may have access to or otherwise Process the Sophos Personal Data and ensure that such Personnel: (i) are informed of the confidential nature of the Sophos Personal Data, (ii) are subject to written confidentiality obligations or professional or statutory obligations of

confidentiality; (iii) comply with the obligations set out in these Data Processing Terms; and (iv) do not publish, divulge, or otherwise disclose any of the Sophos Personal Data to any third party other than in accordance with these Data Processing Terms.

7. SUB-PROCESSORS

7.1. Supplier has Sophos' general authorisation for the engagement of a Sub-Processor, provided that Supplier complies with the requirements set forth herein. Supplier is permitted to use those Sub-processors that Sophos has been notified of by Supplier at the time of execution of the Agreement. Supplier shall specifically inform Sophos in writing of any intended changes to that list through the addition or replacement of Sub-processors at least 30 days in advance, thereby giving Sophos sufficient time to be able to object to such changes prior to the engagement of the Sub-processor(s). The parties will work together in good faith to resolve any such objection, prior to the Processing of Sophos Personal Data by the new Sub-processor. If the parties are unable to resolve such objection, Sophos may terminate the Agreement at no fault by notifying Supplier in writing. Supplier shall provide Sophos with the information necessary to enable Sophos to exercise its right to object.

7.2. Notwithstanding the foregoing authorization, Supplier must (and must ensure that its Sub-processors will):

7.2.1. carry out adequate due diligence to ensure that such Sub-processor is capable of providing the level of protection for Sophos Personal Data required by this Addendum, the Agreement, and the Data Protection Laws and Regulations;

7.2.2. ensure that the arrangement between Supplier and such Sub-processor is governed by a written contract that includes privacy, security and confidentiality requirements and obligations as required by this Addendum, the Agreement, and the Data Protection Laws and Regulations; and

7.2.3. remain fully liable to Sophos for performance of the obligations under these Data Processing Terms, the Agreement and the Data Protection Laws and Regulations.

8. RETENTION; DURATION OF PROCESSING

8.1. Supplier shall securely delete and, at the request of Sophos, return a copy of the Sophos Personal Data at the end of the provision of the Services and/or at any time upon Sophos' written request, except to the extent prohibited from doing so by applicable laws. Supplier shall provide Sophos with written certification of the destruction of the Sophos Personal Data.

8.2. If Supplier is required by applicable laws to retain any Sophos Personal Data, Supplier shall take steps to (i) ensure the continued confidentiality and security of the Sophos Personal Data; (ii) securely delete or destroy the Sophos Personal Data when the legal retention period has expired; and (iii) not actively Process the Sophos Personal Data other than as necessary to comply with such applicable law.

9. TRANSFERS OF SOPHOS PERSONAL DATA

9.1. Restricted Transfers by and between Supplier and any Sub-processor are prohibited, except to the jurisdictions agreed upon in the Agreement or applicable SOW, or otherwise consented to in writing by Sophos. Where Sophos consents to any such Restricted Transfer, it does so subject to

Supplier's compliance with the obligations set out in this Section 9 of these Data Processing Terms.

9.2. Supplier will ensure that any Restricted Transfers by or between Supplier and any Sub-processor comply with applicable Data Protection Laws and Regulations and that, before the commencement of any such Restricted Transfer, the SCCs and as applicable the UK Addendum have been duly and effectively executed between the relevant data importer and data exporter. Upon request, Supplier shall evidence to Sophos that the SCCs are in place with any Sub-processors in respect of such Restricted Transfers.

9.3. With respect to any Restricted Transfers by or on behalf of Sophos to Supplier:

9.3.1. The SCCs and the UK Addendum are expressly incorporated hereto and form a part of these Data Protection Terms;

9.3.2. Subject to Section 9.3.3 and **Exhibit 3** hereto, Supplier and Sophos hereby enter into and agree to: (i) the SCCs, which shall apply to the extent of a Restricted Transfer of Sophos Personal Data by or on behalf of Sophos to Supplier; and (ii) the UK Addendum, which shall apply to, and modify and supplement the SCCs with respect to any Restricted Transfer of Sophos Personal Data that is subject to the Data Protection Laws and Regulations of the United Kingdom; and

9.3.3. For the purposes of the SCCs, Sophos is the data exporter and Supplier is the data importer and a Processor. Where Sophos is a Controller with respect to the Sophos Personal Data (as described in **Attachment A to Exhibit 3**), Module 2 of the SCCs shall apply, subject to the terms of **Exhibit 3** hereto. Where Sophos is a Processor acting on behalf of a Controller with respect to the Sophos Personal Data (as described in **Attachment B to Exhibit 3**), Module 3 of the SCCs shall apply, subject to the terms of **Exhibit 3** hereto.

9.4. Upon request, Supplier will enter into additional agreements with Sophos to (i) adopt the SCCs as necessary for compliance with applicable Data Protection Laws and Regulations; or (2) to adopt an alternative mechanism for (A) establishing appropriate safeguards pursuant to Art. 46 of the GDPR or UK GDPR (as applicable) or (B) the transfer of Company Personal Data on the basis of an adequacy decision pursuant to Art. 45 the GDPR or UK GDPR (as applicable).

10. CHANGES IN DATA PROTECTION LAWS AND REGULATIONS

10.1. If any amendment to these Data Processing Terms is required for compliance with Data Protection Laws and Regulations, then either party may provide written notice to the other party of that change in law. The parties will discuss and negotiate in good faith any necessary variations to these Data Processing Terms to address such changes. The parties will not unreasonably withhold consent or approval to amend this these Data Processing Terms pursuant to this Section 10 or otherwise.

10.2. Supplier agrees that Sophos may, upon prior written notice to Supplier, amend these Data Processing Terms, as follows: (i) in the event the SCCs are replaced, updated or superseded or new or alternative standard contractual clauses for Restricted Transfers are approved by a competent Supervisory Authority ("**New SCCs**"), Supplier agrees that Sophos may update the Agreement and these Data Processing Terms as necessary to incorporate such New SCCs, as an amendment to or replacement of the SCCs; (ii) where Sophos adopts an alternative mechanism

for establishing appropriate safeguards pursuant to Art. 46 of the GDPR or UK GDPR as applicable (such as Binding Corporate Rules), or for the transfer of Company Personal Data on the basis of a valid adequacy decision pursuant to Art. 45 the GDPR or UK GDPR as applicable (such as self-certification to the EU-US and Swiss-US Privacy Shield programs), Sophos may amend and update these Data Processing Terms as necessary to incorporate such alternative mechanism.

11. LIMITATION OF LIABILITY

11.1. The Supplier will indemnify Sophos from and against any and all fines, losses, and/or damages incurred by Sophos and (if applicable) Customers, as a result of the Supplier's breach of these Data Processing Terms or the Data Protection Laws and Regulations.

11.2. The Supplier's liability to Sophos under these Data Processing Terms shall not exceed the greater of:

11.2.1. any limitation or exclusion of liability which applies to the Supplier as set forth in the Agreement; or

11.2.2. the sum of five-million (US) dollars ($5,000,000) per claim.

12. GENERAL

12.1. Sophos and any Sophos Affiliate shall be a beneficiary of these Data Processing Terms.

12.2. Unless a separate Data Processing Agreement has been signed between the parties, these Data Processing Terms shall constitute the entire agreement between the parties in relation to Personal Data collected, processed and used by the Supplier on behalf of Sophos, and shall supersede all previous agreements, arrangements and understandings between the parties in respect of the Processing of Sophos Personal Data.

12.3. These Data Processing Terms shall be governed by and construed in accordance with the laws of England and Wales and the English courts shall have exclusive jurisdiction to determine any disputes which may arise out of, under, or in connection with these Data Processing Terms.

12.4. Without limitation of any other rights available in law or equity, Sophos may seek injunctive relief from any jurisdiction or venue if, in the sole discretion of the Sophos, such measures are deemed appropriate to protect Sophos Personal Data.

12.5. A variation of these Data Processing Terms is valid only if it is in writing and signed on behalf of each party.

12.6. Any failure by either party in exercising its rights, powers, or privileges under these Data Processing Terms shall not act as a waiver, nor shall any single or partial exercise preclude any further exercise of a right, power, or privilege by that party.

12.7. In the event that any provision(s) of these Data Processing Terms are held to be invalid, illegal, or unenforceable, the remaining provisions of these Data Processing Terms shall continue in full force and effect.

12.8. In the event of any conflict or inconsistency between the provisions of the Agreement and these Data Processing Terms: (i) the provisions of these Data Processing Terms shall prevail, unless such other provisions are expressly and specifically stated to have been amended by a provision

in the Agreement or relevant SOW; and (ii) the SCCs and the UK Addendum will, to the extent applicable, prevail in the event of a conflict with any other any provision of these Data Processing Terms.

LIST OF EXHIBITS

Exhibit 1

DETAILS OF THE PROCESSING

1. Categories of data subjects whose personal data is transferred: The Personal Data concern the following categories of data subjects:

    - Prospects, customers, business partners and vendors of Sophos
    - Employees or contact persons of Sophos' prospective customers, customers, business partners and vendors
    - Employees, agents, and contractors of Sophos
    - Other Data Subjects about whom Supplier collects and Processes Personal Data pursuant to the Services

2. Categories of personal data transferred: The Personal Data concern the following categories of data:

    - First and last name
    - Contact information (company, email, phone, physical business address)
    - Employment details such as title, manager's name, salary and benefits
    - Sophos employee dependent and beneficiary information

3. The Personal Data concern the following special categories of data:

    None

4. Nature of the processing:

    Providing the Services purchased by Sophos under and pursuant to the Agreement

5. Purpose(s) of the data transfer and further processing:

    Supplier will process Personal Data as necessary to perform the Services pursuant to the Agreement and as instructed by Sophos in its use of the Services.

SOPHOS
Cybersecurity delivered.

Exhibit 2

TECHNICAL AND ORGANISATIONAL MEASURES

A. Organisational Controls

1. The Supplier shall maintain a written data protection and information security policy.
2. All Supplier's employees and other individuals with access to Sophos Personal Data must be trained on (i) the importance of data protection and information security, (ii) the content of the Supplier's data protection and information security policy, (iii) the Supplier's data protection and information security controls, and (iv) each individual's responsibilities with respect to data protection and information security.
3. The Supplier shall appoint an individual with responsibility for data protection and information security.

B. Business Continuity Measures

1. The Supplier must protect its premises from fire, flood and other environmental hazards.
2. Servers and other critical IT equipment shall be stored in climate-controlled data centres.
3. The Supplier will maintain back-up generators to maintain power supplies in the event of power outages.
4. The Supplier shall maintain a business continuity plan and shall provide a copy for review by Sophos upon request.
5. The Supplier shall test its business continuity plan at least once per annum and shall provide Sophos with the results upon request.

C. Physical Controls

The Supplier shall maintain the following physical controls:

1. Fit appropriate locks or other physical controls to doors and windows;
2. Entry to the Supplier's premises shall be controlled by ID cards with PINs;
3. All visitors shall be required to report to Reception or Security upon arrival;
4. All visitors shall be accompanied by Supplier personnel at all times while on the Supplier's premises;
5. All servers shall be housed in locked cages or locked data rooms with limited access and CCTV surveillance;
6. Use removable media (such as removable hard-drives, CDs and USB sticks) only where essential for the performance of the Agreement;
7. Unattended laptops and removable media must be physically secured (for example by locking away);
8. Permanently and irreversibly erase data from laptops and removable media once the essential purpose has been fulfilled;
9. Permanently and irreversibly erase data from computer equipment before disposal.

D. Testing and Change Control

1. The Supplier shall maintain and apply a change control process for the deployment of new hardware, software, systems and developments.
2. The Supplier shall test all new hardware, software, systems and developments prior to release to the production environment.
3. The production environment must be separate from test systems.
4. Sophos Personal Data may not be used on test systems or for any test purposes unless Sophos expressly agrees otherwise in writing.
5. The Supplier shall verify the success of the deployment into the production environment.

E. Logical Controls

The Supplier shall maintain the following logical controls:

1. Firewalls and intrusion detection mechanisms;
2. Access control approval procedures to ensure that access is only granted to individuals that have an express need for the data;
3. Immediate removal of access rights for individuals that no longer require access or have ceased to be employed/engaged by Supplier;
4. System access and event logging;
5. Fully updated malware and spyware protection;
6. Individual user IDs and strong passwords which are changed at least every 30 days;
7. Encryption of laptops and other removable media;
8. Encryption of data when in transit and at rest;
9. Logical separation of Sophos Personal Data from data belonging to other customers;
10. Remote access must be restricted to authorized individuals via a secure virtual private network.

Exhibit 3

ADDITIONAL TERMS FOR RESTRICTED TRANSFERS

This Exhibit 3 includes additional terms applicable to Restricted Transfers by or on behalf of Sophos to Supplier, pursuant to the Data Processing Terms, as well as the information necessary to complete the Appendices (Annexes I – III) to the applicable SCCs.

By agreeing to the Data Protection Terms, the Parties agree to and thereby execute the SCCs in all relevant parts, subject to Section 9 of the Data Processing Terms and the terms of this Exhibit 3.

1. Capitalized terms used but not defined in this Exhibit 3 or otherwise in the Data Processing Terms, shall have the meanings ascribed to them under the SCCs and the UK Addendum as applicable.

2. Where Sophos is a Controller with respect to the Sophos Personal Data, Module 2 of the SCCs shall apply, subject to the terms of this Exhibit and the Appendix to the SCCs shall be completed with reference to Attachment A hereto.

3. Where Sophos is a Processor acting on behalf of a Controller with respect to the Sophos Personal Data, Module 3 of the SCCs shall apply, subject to the terms of this Exhibit and the Appendix to the SCCs shall be completed with reference to Attachment B hereto.

4. For the purposes of the SCCs (Module 2 and Module 3):

    4.1. Clause 7: the optional docking clause shall not apply;

    4.2. Clause 9(a): Option 2 (General Authorization) shall apply and the data importer shall notify the data exporter in writing at least 30 days in advance of any intended changes.

    4.3. Clause 11: the optional language shall not apply.

    4.4. For purposes of Clause 13(a), the competent supervisory authority shall apply as follows:

        4.4.1. Where the data exporter is established in an EU Member State, the supervisory authority will be the competent supervisory authority for the jurisdiction in which the data exporter is established;

        4.4.2. Where the data exporter is established in the United Kingdom or the Restricted Transfer is subject to the Data Protection Laws and Regulations of the United Kingdom, the competent supervisory authority shall be the UK Information Commissioner's Office;

        4.4.3. Where the data exporter is established in Switzerland or the Restricted Transfer is subject to the Data Protection Laws and Regulations of Switzerland, the Swiss Federal Data Protection and Information Commissioner shall act as the competent supervisory authority; and

        4.4.4. Where the data exporter is not established in an EU Member State, the United Kingdom or Switzerland, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2), the supervisory authority will be the competent supervisory authority for the jurisdiction in which the data exporter's representative is established, namely the Data Protection Commissioner of Ireland.

4.5. For purposes of Clause 17 and Clause 18(b), respectively, the SCC's shall be governed by the laws of the Republic of Ireland disputes will be resolved before the courts of Ireland, except that: (i) where the data exporter is established in Switzerland or the Restricted Transfer is subject to the Data Protection Laws and Regulations of Switzerland, the SCC's shall be governed by the laws of, and disputes will be resolved before the courts of, Switzerland; and (ii) where the data exporter is established in the United Kingdom or the Restricted Transfer is subject to the Data Protection Laws and Regulations of the United Kingdom, the SCC's shall be governed by the laws of, and disputes will be resolved before the courts of, the United Kingdom.

5. **Additional Terms for Switzerland**. Where the data exporter is established in Switzerland or the Restricted Transfer is subject to the Data Protection Laws and Regulations of Switzerland: (i) references in the SCCs to "European Union", "Union" or "member state" shall mean Switzerland; (ii) references to the GDPR shall also include the reference to the equivalent provisions of the Swiss Federal Act on Data Protection (as amended or replaced); and (iii) the SCCs also apply to the transfer of information relating to an identified or identifiable legal entity to the extent such information is protected as Personal Data under the applicable Data Protection Laws and Regulations of Switzerland.

6. **Additional Terms for the United Kingdom**. Where the data exporter is established in the United Kingdom or the Restricted Transfer is subject to the Data Protection Laws and Regulations of the United Kingdom:

   6.1. The SCCs shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK Addendum; and

   6.2. For the purposes of Part One, Tables 1 and Table 2 are completed with reference Attachments A and B (as applicable) of this Exhibit C to the Data Processing Terms, Table 3 is completed with reference to the information in this Exhibit C, and for purposes of Table 4 the data importer may end the UK Addendum as set out in Section 19.

7. **Additional Terms for Processor-to-Processor Restricted Transfers**. The following terms apply only with respect to Restricted Transfers where Sophos is a Processor and the data exporter (Module 3):

   7.1. Supplier shall provide notification to Sophos, and Sophos shall be responsible for notifying the Controller, for the purposes of: (i) Clause 8.6(c) and (d), subject to Section 5 (Breach Notification) of the Data Processing Terms; and (ii) Clause 10, subject to Section 4 (Cooperation and Support) of the Data Processing Terms; and

   7.2. For the purposes of Clause 8.9, enquiries from the relevant Controller shall be provided to Supplier by Sophos as necessary under applicable law.

Attachment A to Exhibit 3

APPENDIX TO THE SCCS (MODULE 2): CONTROLLER-TO-PROCESSOR RESTRICTED TRANSFERS

ANNEX I

A. LIST OF PARTIES

1. Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name	Sophos Limited (for and on behalf of its EU and Swiss subsidiaries
Address	The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Other information needed to identify the Organisation	Registration number 2096520
Contact person's Name: Position: Contact details:	Privacy Counsel dataprotection@sophos.com
Activities relevant to the data transferred under these SCCs	In accordance with the Agreement
Role	Controller

Data Exporter Signature and Date: The SCCs (Module 2), together with this Appendix and the Annexes herein, are executed as part of the Data Processing Terms.

2. **Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*.]

Name	Supplier as set forth under the Agreement
Address	Supplier as set forth under the Agreement
Other information needed to identify the Organisation	Supplier as set forth under the Agreement
Contact person's Name: Position: Contact details:	Supplier as set forth under the Agreement
Activities relevant to the data transferred under these SCCs	The provision of the Services to Sophos pursuant to the Agreement.
Role	Processor

Data Importer Signature and Date: The SCCs (Module 2), together with this Appendix and the Annexes herein, are executed as part of the Data Processing Terms.

B. DESCRIPTION OF TRANSFER

1.1. Categories of *data subjects whose personal data is transferred.*

As set forth in Exhibit 1.

1.2 Categories of *personal data transferred.*

As set forth in Exhibit 1.

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.

None

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

Continuous.

Nature *of the processing*

Providing the Services procured by Sophos under and pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

Supplier will process Sophos Personal Data as necessary to perform the Services pursuant to the Agreement and as instructed by Sophos in its use of the Services.

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

Subject to Section 8 of the Data Processing Terms, Supplier will process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

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

Supplier is authorised the to use the Sub-processors as notified by Supplier to Sophos at the time of execution of the Agreement or the Data Processing Terms.

C. COMPETENT SUPERVISORY AUTHORITY

As set out in Section 4.4 of Exhibit 3 to the Data Processing Terms.

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

Not applicable (Controller has chosen Clause 9 (a), Option 2 of the EU SCC).

ANNEX III – LIST OF SUB-PROCESSORS

Not applicable (The parties have agreed to Option 2 (General Authorization) with respect to Clause 9 (a) of the SCCs).

Attachment B to Exhibit 3

APPENDIX TO THE SCCS (MODULE 3): PROCESSOR-TO-PROCESSOR RESTRICTED TRANSFERS

ANNEX I

A. LIST OF PARTIES

1. Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name	Sophos Limited (for and on behalf of its EU and Swiss subsidiaries)
Address	The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Other information needed to identify the Organisation	Registration number 2096520
Contact person's Name: Position: Contact details:	Privacy Counsel dataprotection@sophos.com
Activities relevant to the data transferred under these SCCs	In accordance with the Agreement
Role	Processor

Data Exporter Signature and Date: The SCCs (Module 2), together with this Appendix and the Annexes herein, are executed as part of the Data Processing Terms.

2. **Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*.]

Name	Supplier as set forth under the Agreement
Address	Supplier as set forth under the Agreement
Other information needed to identify the Organisation	Supplier as set forth under the Agreement
Contact person's Name: Position: Contact details:	Supplier as set forth under the Agreement
Activities relevant to the data transferred under these SCCs	The provision of the Services to Sophos pursuant to the Agreement.
Role	Processor

Data Importer Signature and Date: The SCCs (Module 2), together with this Appendix and the Annexes herein, are executed as part of the Data Processing Terms.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred.

As set forth in Exhibit 1.

Categories of personal data transferred.

As set forth in Exhibit 1.

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.

None

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

Continuous.

Nature of the processing

Providing the Services procured by Sophos under and pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

Supplier will process Sophos Personal Data as necessary to perform the Services pursuant to the Agreement and as instructed by Sophos in its use of the Services.

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

Subject to Section 8 of the Data Processing Terms, Supplier will process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

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

Supplier is authorised the to use the Sub-processors as notified by Supplier to Sophos at the time of execution of the Agreement or the Data Processing Terms.

C. COMPETENT SUPERVISORY AUTHORITY

As set out in Section 4.4 of Exhibit 3 to the Data Processing Terms.

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

Not applicable (Controller has chosen Clause 9 (a), Option 2 of the EU SCC).

ANNEX III – LIST OF SUB-PROCESSORS

Not applicable (The parties have agreed to Option 2 (General Authorization) with respect to Clause 9 (a) of the SCCs).