NOTA: Esta traducción se ha generado de forma automática y se ofrece únicamente para la comodidad de los usuarios. Esta traducción generada automáticamente no ofrece la misma calidad que la traducción humana y puede contener errores. Esta traducción se proporciona "TAL CUAL" y sin ninguna garantía en cuanto a la exactitud, la exhaustividad o la fiabilidad de la misma. Si existiera alguna incoherencia entre la versión en lengua inglesa de este acuerdo y cualquier versión traducida, prevalecerá la versión en lengua inglesa.

ANEXO DE PROCESAMIENTO DE DATOS

Fecha De Revisión: 18 diciembre de 2022

Si este Anexo de Procesamiento de Datos ("Anexo") se incorpora expresamente por referencia en el Acuerdo principal (como se define en la cláusula 2) entre Sophos Limited, una compañía registrada en Inglaterra y Gales número 2096520, con sede en The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, Reino Unido ("Proveedor") y un cliente del Proveedor ("Cliente"), este Anexo forma parte del Acuerdo principal y es efectivo entre el Proveedor y el Cliente.

Los términos en mayúscula utilizados en este Anexo se definen como se establece en la cláusula 2 a continuación. A petición, podemos proporcionar una copia de este Anexo en otro idioma. En caso de conflicto, prevalecerá la versión en inglés del Anexo.

1. PREÁMBULO

1.1. Las partes han firmado el Acuerdo Principal en relación con la provisión por parte del Proveedor al Cliente de determinados productos y/o servicios (colectivamente, "Productos").

1.2. Si el Acuerdo principal es un Acuerdo de MSP de forma similar al Acuerdo de MSP ubicado en https://www.sophos.com/es-es/legal/sophos-msp-partner-terms-and-conditions ("MSP Acuerdo"), el Cliente es un proveedor de servicios gestionados ("MSP"). Si el Acuerdo Principal es un Acuerdo OEM bajo el cual el Cliente está autorizado a distribuir, sublicenciar o poner a disposición de los Productos Proveedores de terceros en combinación con los productos del Cliente como parte de una unidad empaquetada ("Acuerdo OEM"), el Cliente es un fabricante de equipos originales ("OEM"). De lo contrario, el cliente es un usuario final ("Usuario final").

1.3. La provisión de los Productos puede incluir la recopilación, el uso y otro procesamiento de los Datos Personales del Controlador por parte del Proveedor en nombre del Cliente. El presente Addendum establece las obligaciones de las partes con respecto a dicho procesamiento y complementa los términos y condiciones del Acuerdo Principal.

1.4. Sin perjuicio de cualquier otro término del Acuerdo o de este Anexo, las partes acuerdan que los Datos Personales del Controlador no incluirán información de contacto, información de pago o facturación u otros Datos Personales sobre contactos comerciales y administradores del Cliente, incluidos el nombre, la dirección de correo electrónico y la información de contacto, Qué proveedor recopila y procesa en su propio nombre para gestionar sus relaciones con los clientes, comunicarse con clientes actuales, antiguos y potenciales y socios comerciales, y administrar sus relaciones comerciales ("Datos CRM").

1.4.1. El Proveedor es un Controlador de Datos de CRM y procesará los datos de CRM de acuerdo con sus obligaciones bajo la Ley de Protección de Datos aplicable y el Aviso de Privacidad del Grupo de Proveedores.

1.4.2. Excepto en lo que respecta a la Sección 1.4.1, las obligaciones del Proveedor en virtud de este Anexo no se aplicarán a los Datos de CRM.

1.5. El Acuerdo Principal, este Anexo y los documentos a los que se hace referencia expresamente en el Acuerdo Principal y este Anexo constituirán el Acuerdo completo entre las partes en relación con los datos personales recopilados, procesados y utilizados por el Proveedor en nombre del Cliente en relación con el Acuerdo Principal, y reemplazará todos los acuerdos, arreglos y entendimientos anteriores entre las partes con respecto a ese tema.

2. DEFINICIONES

2.1. En este Anexo, los siguientes términos tendrán los siguientes significados:

Por «Leyes aplicables de protección de datos» se entenderá, en la medida aplicable: (a) el Reglamento 2016/679 de la UE del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos (Reglamento general de protección de datos o «GDPR»); (b) la Directiva sobre privacidad electrónica (Directiva 2002/58/CE de la UE); y (c) toda la legislación nacional aplicable sobre protección de datos, incluida la legislación que se haya establecido en virtud de (a) o (b); en cada caso que pueda modificarse o sustituirse de vez en cuando.

“Beneficiario” tiene el significado que se le da en el MSP Acuerdo.

“CCPA” se refiere a la Ley de Privacidad del Consumidor de California (California Consumer Privacy Act), enmendada por la Ley de Derechos de Privacidad de California de 2020), codificada en Cal. Civ. Artículo 1798.100 - 1798.199.100 del Código y las Regulaciones de la Ley de Privacidad del Consumidor de California emitidas al mismo, Cal. Registro de códigos tit. 11, div. 6, ch. 1, cada uno según sus modificaciones;

“Cláusulas” tendrán el significado que se le atribuye en las SCC.

“Controlador” significa: (a) el Cliente, si el Cliente es un Usuario Final; (b) el Beneficiario, si el Cliente es un MSP; o (c) el Cliente Final, si el Cliente es un OEM.

“Datos personales del controlador” se refiere a los Datos personales que el Proveedor procesa en nombre del controlador de conformidad con los Servicios.

“Cláusulas del Controlador al Procesador” significa las Cláusulas del Módulo Dos de las SCC. “Datos CRM” significa información de contacto, información de pago o facturación u otros Datos personales sobre contactos comerciales y administradores del Cliente, incluidos el nombre, la dirección de correo electrónico y la información de contacto, Qué proveedor recopila y procesa en su propio nombre con el fin de gestionar sus relaciones con los clientes, comunicarse con clientes actuales, antiguos y potenciales y socios comerciales, y administrar sus relaciones comerciales.

“Sujeto de datos” significa la persona con la que se relacionan los Datos personales de Sophos.

“Solicitudes del interesado” significa cualquier solicitud de los interesados que ejerzan derechos de conformidad con las leyes de protección de datos aplicables, incluidos sus derechos de acceso, eliminación y corrección.

“EEE” significa el Espacio Económico Europeo, incluidos (a) los Estados miembros del Espacio Económico Europeo (“EEE”) y (b) el Reino Unido.

“Cliente final” tiene el significado que se le da en el Acuerdo del OEM.

«Europa» (y «Europa») significa (a) los Estados miembros del Espacio Económico Europeo («EEE») y (b) el Reino Unido.

“ Productos alojados” se refiere a los productos enumerados en el Anexo 3.

“ICO” significa la Oficina del Comisionado de Información establecida en el Reino Unido

“Acuerdo principal” se refiere, colectivamente, al acuerdo(s) escrito(s), incluyendo y exhibe, anexos y enmiendas al mismo, de conformidad con el cual el Proveedor proporciona ciertos Servicios al Cliente.

“Datos personales” significa cualquier información que identifique, pueda utilizarse para identificar o esté vinculada o razonablemente vinculada con un individuo o un hogar en particular, así como cualquier información definida como “datos personales”, “información personal” o término equivalente en virtud de las leyes y reglamentos de protección de datos aplicables.

“Incumplimiento de datos personales” se refiere a un incumplimiento de la seguridad (distinto de los causados por el Cliente o sus usuarios) que lleve a la destrucción, pérdida, alteración, divulgación o acceso accidentales o ilegales a, Datos personales del controlador procesados por el Proveedor en virtud de este Anexo.

“Procesador” significa una persona o entidad que procesa Datos Personales en nombre y bajo las instrucciones del Controlador, incluida cualquier entidad que actúe como “proveedor de servicios” de conformidad con la CCPA.

“Transferencia Restringida” significa una transferencia de Datos Personales del Controlador por parte del Cliente al Proveedor, cuando dicha transferencia estaría prohibida por las Leyes de Protección de Datos aplicables en ausencia de las Cláusulas Contractuales Estándar aplicables y, en su caso, el Apéndice del Reino Unido.

“Datos sensibles” significa “categorías especiales de datos personales”, “datos personales sensibles”, “datos sensibles” y término equivalente según se define en las leyes de protección de datos aplicables.

“Servicios” se refiere a todos y cada uno de los productos proporcionados y/o servicios prestados por el Proveedor de conformidad con el Acuerdo principal.

Por “cláusulas contractuales estándar” o “SCC” se entiende las cláusulas contractuales estándar para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo aprobado por la decisión de aplicación de la Comisión Europea (UE) 2021/914 de 4 de junio de 2021.

"Subprocesador" significa cualquier persona o entidad (excluyendo cualquier empleado del Proveedor) o entidad designada por o en nombre del Proveedor que procesa Datos Personales del Controlador.

"Autoridad de Supervisión" significa la autoridad reguladora competente con respecto a las leyes y reglamentos de protección de datos aplicables, incluida, cuando corresponda, una autoridad supervisora según se define en el RGPD.

"Adenda del Reino Unido" significa el Adenda de Transferencia Internacional de Datos a las Cláusulas Contractuales Estándar de la Comisión de la UE, emitido por la ICO, en su versión modificada o reemplazada de vez en cuando por una Autoridad de Supervisión competente en virtud de las leyes de protección de datos pertinentes del Reino Unido

2.2. En este Anexo, los términos en minúsculas «controlador», «procesador», «asunto de los datos», «datos personales» y «procesamiento» (y sus derivados) tendrán los significados que se indican en la Ley de protección de datos aplicable.

3. ALCANCE

3.1. El objeto y la duración del tratamiento de los Datos personales del controlador por parte del Proveedor, incluida la naturaleza y el propósito del procesamiento, los tipos de Datos personales del controlador que se van a procesar y las categorías de sujetos de los datos, serán los descritos en: (a) este Anexo; (b) el Acuerdo principal; (c) cualquier instrucción en el Anexo 1 (Instrucciones de procesamiento de datos); y (d) las instrucciones del Cliente emitidas de acuerdo con la cláusula 4 a continuación.

3.2. El Cliente es responsable de garantizar (a) que el Controlador tiene una base legal para el procesamiento de los Datos Personales del Controlador que será llevado a cabo por el Proveedor en nombre del Cliente, y (b) que el Controlador ha obtenido todos los consentimientos necesarios de los sujetos de datos que puedan ser necesarios para el procesamiento de los Datos Personales del Controlador por el Cliente y el Proveedor (incluyendo, pero sin limitación, en relación con los Datos Sensibles); y (c) que cumpla de otro modo, y se asegurará de que sus instrucciones al Proveedor para el procesamiento de los Datos Personales del Controlador cumplan en todos los aspectos con las Leyes de Protección de Datos aplicables.

3.3. Las partes acuerdan que el Proveedor es un Procesador o Subprocesador para los Datos Personales del Controlador, y el Cliente es (a) el Controlador cuando el Cliente es un Usuario Final, o (b) un Procesador ((para un controlador externo) cuando el Cliente es un MSP u OEM.

4. INSTRUCCIONES PARA EL CLIENTE

4.1. El Cliente instruye al Proveedor que procese los Datos Personales del Controlador según sea razonablemente necesario para proporcionar y realizar los Servicios y según se establezca de otra manera en el presente y en el Acuerdo principal. El Proveedor procesará los Datos Personales del Controlador de acuerdo con las instrucciones de procesamiento documentadas del Cliente, como se indica en el presente documento, excepto (a) cuando se acuerde lo contrario por escrito entre el Proveedor y el Cliente; O (b) cuando lo exija la ley a la que esté sujeto el Proveedor (en cuyo

caso, el Proveedor informará al Cliente de dicho requisito legal antes del procesamiento, a menos que esa ley prohíba el suministro de dicha información).

4.2. Si el Proveedor se da cuenta de que las instrucciones de procesamiento del Cliente infringen las leyes de protección de datos aplicables (sin imponer ninguna obligación al Proveedor de supervisar activamente el cumplimiento del Cliente), notificará inmediatamente al Cliente lo mismo y suspenderá el procesamiento de los Datos personales del controlador.

4.3. Sin limitar lo anterior, en la medida en que la Ley de Privacidad del Consumidor de California ("**CCPA**") se aplique a los Datos Personales del Controlador, el Proveedor acepta además que:

4.3.1. El Proveedor no utilizará, divulgará ni procesará de otra manera los Datos Personales del Controlador, excepto para el propósito específico de realizar los Servicios, de acuerdo con los términos de este Anexo y el Acuerdo principal, y según lo exijan las leyes aplicables. Sin perjuicio de lo anterior:

a. El Proveedor puede contratar a Subprocesadores para procesar Datos Personales del Controlador, sujeto a los términos de la Sección 7;

b. El Proveedor no procesará los Datos Personales del Controlador fuera de la relación comercial directa entre el Cliente y el Proveedor o para fines comerciales propios del Proveedor; No obstante lo anterior, las Partes acuerdan que, en la medida en que se aplique la CCPA, el Proveedor solo procesará los Datos Personales del Controlador para los fines comerciales específicos establecidos en la Acuerdo principal y este Anexo o para otro propósito expresamente autorizado de conformidad con las regulaciones de la CCPA.

c. El Proveedor no "compartirá" ni "venderá" (como esos términos se definen en la CCPA) ningún dato personal del controlador;

d. El Proveedor (y procurará que cada Subprocesador) cumpla con sus obligaciones de conformidad con la CCPA y proporcionará el mismo nivel de protección de la privacidad que requiere la CCPA; y.

e. Si el Proveedor cree que no podrá cumplir con los términos de este Anexo o con las Leyes de Protección de Datos aplicables, El Proveedor notificará inmediatamente al Cliente y le otorgará al Cliente el derecho de tomar medidas razonables y apropiadas para garantizar que los Datos Personales del Controlador se procesen de una manera que sea consistente con las obligaciones del Controlador bajo la CCPA.

f. El Proveedor no conservará los Datos Personales del Responsable del Tratamiento al vencimiento o terminación del Acuerdo principal, excepto en los casos establecidos en la Sección **Error! Reference source not found.**;

5. OBLIGACIONES DEL PROVEEDOR

5.1. Todo el personal del Proveedor que procese los Datos personales del controlador deberá estar debidamente formado con respecto a sus obligaciones de protección de datos, seguridad y confidencialidad, y estará sujeto a obligaciones escritas o legales para mantener la confidencialidad.

5.2. El Proveedor implementará las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo y proteger los Datos personales del controlador contra una Incumplimiento de Datos Personales. Tales medidas tendrán en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines de la tramitación, así como el riesgo de que varyan las probabilidades y la severidad de los derechos y libertades de las personas físicas, a fin de garantizar un nivel de seguridad adecuado al riesgo. En particular, las medidas adoptadas por el Proveedor incluirán las descritas en el Anexo 2 del presente Anexo. El Proveedor puede cambiar o modificar las medidas técnicas y organizativas descritas en el Anexo 2 sin el consentimiento previo por escrito del Cliente, siempre que el Proveedor mantenga al menos un nivel de protección equivalente. A petición del Cliente, el Proveedor proporcionará una descripción actualizada de las medidas técnicas y organizativas en el formulario que se presenta en el Anexo 2.

5.3. El Proveedor deberá seguir los requisitos especificados en la cláusula 7 a continuación para contratar a cualquier Subprocesador para procesar Datos Personales del Controlador.

5.4. El Proveedor seguirá los requisitos especificados en la Cláusula 8 a continuación para ayudar al Cliente a responder a consultas de terceros, incluidas las solicitudes de los sujetos de datos para ejercer sus derechos conforme a las leyes de protección de datos aplicables.

5.5. Al confirmar la aparición de cualquier violación de los datos personales, el Proveedor informará al Cliente sin demora indebida y proporcionará toda la información y cooperación oportunas que el Cliente pueda requerir razonablemente para el Cliente (y, si el Cliente es un MSP o OEM, su Controlador) Cumplir sus obligaciones de notificación de infracciones de datos en virtud de (y de acuerdo con los plazos exigidos por) la Ley de protección de datos aplicable. Además, el Proveedor tomará las medidas y acciones que sean razonablemente necesarias para remediar o mitigar los efectos de la violación de datos personales y mantendrá al Cliente informado de la evolución en relación con la violación de datos personales.

5.6. El Proveedor proporcionará al Cliente (o, si el Cliente es un MSP u OEM, su Controlador) una asistencia razonable y oportuna como el Cliente (o, según corresponda, el Controlador). Puede requerir para llevar a cabo una evaluación de impacto de la protección de datos u otra evaluación que sea requerida por las leyes de protección de datos aplicables y, si es necesario, consultar con su autoridad de protección de datos pertinente. Dicha asistencia se proporcionará a expensas del Cliente.

5.7. El Proveedor, a menos que la ley aplicable exija lo contrario, eliminará los Datos Personales del Controlador dentro de un período de tiempo razonable después de la terminación o vencimiento de este Anexo, a menos que lo prohíba la ley aplicable. Previa solicitud, el Proveedor confirmará al Cliente que dichos Datos Personales del Controlador han sido eliminados de acuerdo con este Anexo. Si las leyes aplicables exigen al Proveedor que conserve cualquier dato personal del Controlador, el Proveedor tomará medidas para garantizar la confidencialidad y seguridad continuas de los datos personales del Controlador durante el tiempo que se mantengan.

6. DERECHOS DE AUDITORÍA DEL CLIENTE

6.1. El Cliente reconoce que el Proveedor es auditado regularmente de conformidad con las normas SSAE 18 SOC 2 por auditores independientes de terceros. Previa solicitud razonable, el Proveedor deberá proporcionar al Cliente una copia de su informe de auditoría del SOC 2, que estará sujeta a las disposiciones de confidencialidad del Acuerdo Principal como información confidencial del Proveedor. El Proveedor también responderá a cualquier pregunta razonable de auditoría por escrito que le envíe el Cliente, siempre que el Cliente no ejerza este derecho más de una vez al año.

6.2. Si, en opinión razonable del Cliente, los materiales proporcionados en virtud de la cláusula 6.1 son insuficientes para demostrar el cumplimiento del Proveedor con este Apéndice, el Cliente puede solicitar por escrito y sujeto a la cláusula 6.2 (a) - (d) del presente documento, Que el Proveedor ponga a disposición del Cliente toda la información razonablemente necesaria para demostrar el cumplimiento de las obligaciones establecidas en este Anexo (incluidas las Cláusulas Contractuales Estándar en la medida en que sean aplicables) y permita y contribuya a auditorías, incluidas inspecciones, por parte del Cliente o por parte del Cliente independiente, Auditor externo que no sea un competidor del Proveedor de las Actividades de Procesamiento que están cubiertas por este Anexo.

a. Antes de solicitar una revisión o auditoría de conformidad con esta cláusula 6.2, el Cliente tendrá en cuenta las certificaciones y auditorías de terceros del Proveedor pertinentes descritas en la cláusula 6.1;

b. El Cliente notificará al Procesador con una antelación razonable, con al menos 60 días de antelación, una solicitud para llevar a cabo una auditoría o inspección en virtud de esta cláusula 6.2. y tomará (y se asegurará de que cada uno de sus auditores tome) medidas razonables para evitar y prevenir cualquier daño o lesión y minimizar cualquier interrupción de dicha auditoría o inspección;

c. Una auditoría o inspección no se llevará a cabo más de una vez al año, excepto cuando sea requerido por una Autoridad de Supervisión o las Leyes de Protección de Datos aplicables; y

d. El Cliente asumirá todos los costos de dicha auditoría y reembolsará al Proveedor los costos y gastos razonables incurridos por el Proveedor de conformidad con dichas auditorías, incluido cualquier tiempo invertido por el Proveedor, sus Afiliados o sus Subprocesadores para cualquier auditoría o inspección a las tarifas de servicios profesionales vigentes en ese momento del Proveedor, Que se pondrá a disposición del Cliente a petición.

7. SUB

7.1. El Cliente acepta el uso de los Subprocesadores existentes del Proveedor a la fecha de este Anexo, que se enumeran enhttps://www.sophos.com/es-es/legal(“Lista de Subprocesadores”), así como las Afiliadas del Proveedor. El Cliente consiente expresamente la contratación por parte del Proveedor de Subprocesadores de terceros adicionales (cada uno de ellos un “Nuevo Subprocesador”) sujeto a los términos establecidos en esta cláusula 7. El Proveedor proporcionará al Cliente un aviso de treinta (30) días antes de la adición de cualquier Nuevo Subprocesador, el

cual puede ser notificado mediante la publicación de los detalles de dicha adición a la Lista de Subprocesadores.

7.2. Si el Cliente no se opone por escrito a la designación de un nuevo subprocesador por parte del Proveedor (por motivos razonables relacionados con la protección de los Datos personales del controlador) en un plazo de 30 días desde que el Proveedor agregue dicho nuevo subprocesador a la Lista de subprocesadores, El Cliente acepta que se considerará que ha dado su consentimiento a ese Nuevo Subprocesador. Si el Cliente presenta dicha objeción por escrito al Proveedor, el Proveedor notificará por escrito al Cliente en un plazo de 30 días que: (a) el Proveedor no utilizará el Nuevo Subprocesador para procesar los Datos personales del controlador; o (b) el Proveedor no puede o no está dispuesto a hacerlo. Si se da la notificación que figura en el apartado (b), el Cliente podrá, en un plazo de 30 días a partir de dicha notificación, Elegir rescindir este Anexo y el Acuerdo Principal en cuanto al procesamiento afectado previa notificación por escrito al Proveedor y al Proveedor sólo para los clientes ubicados dentro del Área Económica Europea y Reino Unido, autorizar un reembolso prorrateado o crédito de cualquier tarifa prepagada por el período restante después de la terminación. Sin embargo, si no se proporciona dicho aviso de terminación dentro de ese plazo, se considerará que el Cliente ha dado su consentimiento al Nuevo Subprocesador. El Proveedor impondrá condiciones de protección de datos a los Nuevos Subprocesadores que impondrán protecciones equivalentes para los Datos Personales del Controlador según lo dispuesto en este Anexo. El Proveedor seguirá siendo plenamente responsable del cumplimiento de las obligaciones de cada Subprocesador.

8. INVESTIGACIONES DE TERCEROS

8.1. El Proveedor notificará al Cliente cualquier solicitud de privacidad, correspondencia, consulta o queja que reciba de un sujeto de datos, regulador u otro tercero en relación con el procesamiento de los Datos personales del Controlador proporcionando detalles completos de los mismos, pero no responderá directamente al sujeto de datos. excepto cuando la ley exija lo contrario.

8.2. En la medida en que sea necesario, el Proveedor proporcionará asistencia razonable y oportuna al Cliente (o, si el Cliente es un MSP u OEM, el Controlador), a expensas del Cliente, para permitir al Cliente (o si el Cliente es un MSP u OEM, el Controlador) responder a: (a) una solicitud de un interesado para ejercer sus derechos en virtud de la Ley de Protección de Datos aplicable (incluidos, en su caso, sus derechos de acceso, rectificación, oposición, supresión y portabilidad de datos, As y (b) una solicitud recibida de un regulador u otro tercero en relación con el procesamiento de los Datos personales del controlador.

9. TRANSFERENCIAS INTERNACIONALES DE DATOS

9.1. Ciertos Productos pueden permitir al Cliente seleccionar dónde alojar los Datos Personales del Controlador para dichos Productos, incluidos los centros de datos que pueden estar ubicados fuera de la jurisdicción en la que se originan los datos. Estas ubicaciones pueden incluir (a) el Espacio Económico Europeo, (b) el Reino Unido, (c) los Estados Unidos de América; u otra ubicación según se especifica en el Acuerdo principal (“Ubicación de almacenamiento central”). Esta selección se realiza en el punto de instalación del Producto, creación de cuenta o primer uso del Producto

correspondiente. Una vez seleccionada, la ubicación de almacenamiento central no se puede modificar en una fecha posterior.

9.2. El Cliente reconoce y consiente expresamente, independientemente de la Ubicación Central de Almacenamiento seleccionada (si procede), las Transferencias Restringidas, sujeto al cumplimiento de las obligaciones establecidas en esta cláusula 9.

9.3. Con respecto a cualquier transferencia restringida:

9.3.1. Las SCCs y el Apéndice del Reino Unido se incorporan expresamente al presente y forman parte de este Apéndice;

9.3.2. Sujeto a la Sección 9.3.3 y al Anexo 4 del presente documento, el Cliente y el Proveedor acuerdan: (i) las SCC, que se aplicarán en la medida de una transferencia restringida de datos personales del controlador al proveedor; y (ii) el Apéndice del Reino Unido, que se aplicará a, y modificará y complementará las SCC con respecto a cualquier transferencia restringida de datos personales del controlador que esté sujeta a las leyes y reglamentos de protección de datos del Reino Unido; y

9.3.3. Se aplicará el módulo 2 de los SCC, sujeto a los términos del Anexo 4 del presente documento.

9.4. El apéndice de las SCC se completará como se indica en el Anexo 4.

10. DURACIÓN

10.1. Este Anexo comienza con (a) la ejecución por ambas partes del Acuerdo principal o (b) la fecha en la que el Acuerdo principal entra en vigor, si es posterior y continúa hasta el principio de: (i) la expiración del derecho del Cliente a utilizar y recibir los Productos, tal como se indica en el Acuerdo Principal o en cualquier derecho de licencia asociado; y (ii) la terminación del Acuerdo Principal.

11. OTRAS REGULACIONES

11.1. Las modificaciones y enmiendas a este Apéndice requieren el formulario escrito. Esto también se aplica a los cambios y modificaciones de esta cláusula11.1.

11.2. En ningún caso la responsabilidad del Proveedor con respecto al Cliente en relación con cualquier problema que surja de, o en relación con, este Anexo excederá las limitaciones de responsabilidad del Proveedor establecidas en el Acuerdo Principal. Las limitaciones de responsabilidad del Proveedor, tal como se establecen en el Acuerdo Principal, se aplicarán en conjunto tanto en el Acuerdo Principal como en este Anexo, de forma que se aplique una única limitación del régimen de responsabilidad tanto en el Acuerdo Principal como en este Anexo.

11.3. Este Anexo (excluyendo las SCC) se regirá e interpretará de acuerdo con las leyes de Inglaterra y Gales, sin tener en cuenta los principios de conflicto de leyes. En la medida en que lo permita la ley aplicable, los tribunales de Inglaterra tendrán jurisdicción exclusiva para determinar cualquier disputa o reclamación que pueda surgir de, bajo o en relación con este Apéndice.

11.4. En la medida en que exista un conflicto con los términos de este Anexo de procesamiento de datos y los términos de cualquier SCC celebrado por las partes, los términos de los SCC aplicables (incluidos los anexos de los mismos), tendrán prioridad.

12. CAMBIOS EN LA LEY

12.1. Si se requiere alguna modificación a este Apéndice como resultado de un cambio en las leyes de protección de datos aplicables, cualquiera de las partes puede notificar por escrito a la otra parte de dicho cambio en la ley. Las partes discutirán y negociarán de buena fe cualquier variación necesaria a este Apéndice para abordar dichos cambios. Las partes no rechazarán de manera injustificada el consentimiento o la aprobación para enmendar este Apéndice de conformidad con esta Sección 12 o de otra manera.

12.2. En el caso de que las Cláusulas Contractuales Estándar o el Apéndice del Reino Unido sean reemplazados, actualizados o sustituidos por una nueva versión (“Cláusulas Nuevas”), el Cliente acepta que el Proveedor podrá, previa notificación por escrito al Cliente, actualizar este Apéndice según sea necesario para incorporar dichas Cláusulas Nuevas, Como una modificación o sustitución de las Cláusulas Contractuales Estándar anteriores o el Anexo del Reino Unido.

Anexo 1

DESCRIPCIÓN DEL PROCESAMIENTO

En este Anexo 1 se describe el procesamiento que el Proveedor realizará en nombre del Cliente.

(a) Objeto, naturaleza y finalidad de las operaciones de transformación

Los Datos personales del controlador estarán sujetos a las siguientes actividades básicas de procesamiento (especifíquense):

- Suministro de los Productos comprados por el Cliente bajo y de conformidad con el Acuerdo Principal
- Proporcionar servicios de gestión de cuentas y asistencia técnica al cliente

El Proveedor proporciona Productos diseñados para detectar, prevenir y gestionar, o ayudar al Proveedor a detectar, prevenir y gestionar amenazas de seguridad dentro o contra sistemas, redes, dispositivos, archivos y otros datos disponibles por el Cliente. El contenido de cualquier información contenida en estos sistemas, redes, dispositivos, archivos y otros datos está determinado exclusivamente por el Cliente y no por el Proveedor.

(b) Duración de las operaciones de procesamiento:

Los Datos personales del controlador se procesarán durante la siguiente duración (especifique):

La duración especificada en el Acuerdo principal (o para el término del Acuerdo principal, si no se especifica lo contrario).

(c) Temas de datos

Los Datos personales del controlador se refieren a las siguientes categorías de sujetos de datos (especifique):

- Personal y usuarios finales de clientes
- Otros sujetos de datos cuyos datos personales se procesan en nombre del cliente en relación con los productos de Sophos

(d) Tipos de datos personales

Los Datos personales del controlador se refieren a las siguientes categorías de datos (especifique):

- Nombres de usuario y otros identificadores
- Información de la red y de la actividad de la red
- Otra información que puede transmitirse o procesarse en relación con los Productos de Sophos

(e) Categorías especiales de datos (si procede)

Los Datos personales del controlador se refieren a las siguientes categorías especiales de datos (especifique):

A menos que se especifique lo contrario, los Productos del Proveedor no están diseñados para procesar categorías especiales de datos.

Anexo 2

MEDIDAS TÉCNICAS Y ORGANIZATIVAS

Algunas de estas medidas sólo pueden ser pertinentes o aplicables a los productos alojados.

1. Control de acceso físico.
   (a) Sophos tiene una política de control de acceso físico;
   (b) todo el personal lleva identificación / tarjetas de acceso;
   (c) las entradas a las instalaciones están protegidas por tarjetas de acceso o llaves;
   (d) las instalaciones están divididas en (i) áreas de acceso público (tales como áreas de recepción), (ii) áreas de acceso general del personal, Y (iii) áreas de acceso restringido a las que solo puede acceder el personal con una necesidad comercial expresa;
   (e) Las tarjetas de acceso y las llaves controlan el acceso a las áreas restringidas dentro de cada instalación de acuerdo con los niveles de acceso autorizados de una persona;
   (f) Los niveles de acceso para las personas están aprobados por miembros del personal senior y se verifican trimestralmente;
   (g) el personal de recepción y/o seguridad está presente en las entradas a sitios más grandes;
   (h) Las instalaciones están protegidas por alarmas;
   (i) los visitantes están pre-registrados y se mantienen los registros de visitantes.

2. Control de acceso al sistema.
   (a) Sophos tiene una política lógica de control de acceso;
   (b) la red está protegida por firewalls en cada conexión a Internet;
   (c) la red interna está segmentada por firewalls en función de la sensibilidad de la aplicación;
   (d) IDS y otros controles de detección y bloqueo de amenazas se ejecutan en todos los firewalls;
   (e) El filtrado del tráfico de red se basa en reglas que aplican el principio de “acceso mínimo”;
   (f) los derechos de acceso solo se otorgan al personal autorizado en la medida y durante el tiempo necesario para desempeñar sus funciones laborales y se revisan trimestralmente;
   (g) el acceso a todos los sistemas y aplicaciones está controlado por un procedimiento de inicio de sesión seguro;
   (h) las personas tienen ID de usuario y contraseñas únicas para su propio uso;
   (i) las contraseñas se someten a pruebas de fuerza y se aplican cambios a contraseñas débiles;
   (j) las pantallas y sesiones se bloquean automáticamente después de un período de inactividad;
   (k) Los productos de protección contra malware de Sophos se instalan de forma estándar;
   (l) se realizan análisis periódicos de vulnerabilidades en direcciones IP y sistemas;
   (m) se aplican parches a los sistemas en un ciclo regular con un sistema de priorización para realizar un seguimiento rápido de parches urgentes.

3. Control de acceso a datos.
   (a) Sophos tiene una política lógica de control de acceso;
   (b) los derechos de acceso solo se conceden al personal autorizado en la medida y durante el tiempo necesario para desempeñar sus funciones de trabajo y se revisan trimestralmente;
   (c) el acceso a todos los sistemas y aplicaciones se controla mediante un procedimiento de inicio de sesión seguro;
   (d) las personas tienen ID de usuario y contraseñas únicas para su propio uso;
   (e) las contraseñas se someten a pruebas exhaustivas y se aplican cambios a las contraseñas débiles;
   (f) las pantallas y las sesiones se bloquean automáticamente después de un período de inactividad;
   (g) los ordenadores portátiles se cifran mediante productos de cifrado de Sophos;
   (h) Los remitentes deben considerar el cifrado de archivos antes de enviar cualquier correo electrónico externo.

4. Control de entrada.
   (a) el acceso a todos los sistemas y aplicaciones está controlado por un procedimiento de inicio de sesión seguro;
   (b) las personas tienen ID de usuario y contraseñas únicas para su propio uso;
   (c) los Productos Sophos Central utilizan cifrado de capa de transferencia para proteger los datos en tránsito;
   (d) La comunicación entre el software cliente y el sistema backend Sophos se realiza a través de HTTPS para proteger los datos en tránsito, estableciendo comunicación de confianza a través de certificados y validación del servidor.

5. Control de Subcontratistas.
   (a) los subcontratistas con acceso a los datos emprenden un procedimiento de verificación de LA seguridad de TI antes de la incorporación y según sea necesario posteriormente;
   (b) los contratos contienen una confidencialidad adecuada y obligaciones de protección de datos basadas en las obligaciones del subcontratista.

6. Control de disponibilidad.
   (a) Sophos protege sus instalaciones contra incendios, inundaciones y otros peligros ambientales;
   (b) hay generadores de reserva disponibles para mantener el suministro eléctrico en caso de cortes de energía;
   (c) Los centros de datos y las salas de servidores utilizan controles climáticos y monitoreo;
   (d) El sistema Sophos Central está equilibrado de carga y tiene conmutación por error entre tres sitios, cada uno ejecutando dos instancias del software, cualquiera de los cuales es capaz de proporcionar el servicio completo.

7. Control de segregación.
   (a) Sophos mantiene y aplica un proceso de control de calidad para el despliegue de nuevos productos de clientes;
   (b) Los entornos de pruebas y producción son independientes;
   (c) El nuevo software, sistemas y desarrollos se prueban antes de su lanzamiento al entorno de producción.

8. Control organizacional.
   (a) Sophos cuenta con un equipo de seguridad de TI dedicado;
   (b) el equipo de riesgos y cumplimiento gestiona los informes y controles de riesgos internos, que incluyen informes sobre riesgos clave para la gestión;
   (c) un proceso de respuesta a incidentes identifica y soluciona los riesgos y vulnerabilidades de forma oportuna;
   (d) cada nuevo empleado realiza formación sobre protección de datos y seguridad DE TI;
   (e) el departamento de seguridad de TI lleva a cabo campañas trimestrales de concienciación sobre seguridad.

Anexo 3

PRODUCTOS ALOJADOS

(a) Sophos Central
(b) Sophos Cloud Optix
(c) Central Device Encryption
(d) Central Endpoint Protection
(e) Central Endpoint Intercept X
(f) Central Endpoint Intercept X Advanced
(g) Central Mobile Advanced
(h) Central Mobile Standard
(i) Central Phish Threat
(j) Central Intercept X Advanced for Server
(k) Central Server Protection
(l) Central Mobile Security
(m) Central Web Gateway Advanced
(n) Central Web Gateway Standard
(o) Central Email Standard
(p) Central Email Advanced
(q) Central Wireless Standard
(r) Cualquier otro producto de Sophos Que se administra y opera a través de Sophos Central

Anexo 4

TÉRMINOS ADICIONALES PARA TRANSFERENCIAS RESTRINGIDAS

Este Anexo incluye términos adicionales aplicables a las Transferencias Restringidas por o en nombre del Cliente al Proveedor, de conformidad con el Anexo, así como la información necesaria para completar los Apéndices (Anexos I – III) de los SCC aplicables.

Al aceptar el Anexo, las Partes acuerdan y, por lo tanto, ejecutan los SCC en todas las partes pertinentes, con sujeción a la Sección **Error! Reference source not found.**del Anexo y los términos de este Anexo.

1. Los términos en mayúscula utilizados pero no definidos en este Anexo o de otro modo en el Anexo, tendrán los significados que se les atribuyen en virtud de los SCC y el Anexo del Reino Unido, según corresponda.

2. Se aplicará el módulo 2 de los SCC, sujeto a los términos de este Anexo y el Apéndice de los SCC se completará con referencia al Anexo A del presente Reglamento.

3. Para los fines de los SCCs (Módulo 2):

3.1. Cláusula 7: No se aplicará la cláusula de acoplamiento opcional;

3.2. Cláusula 9(a): Se aplicará la opción 2 (Autorización general) y el importador de datos notificará al exportador de datos por escrito con al menos 30 días de anticipación de cualquier cambio previsto.

3.3. Cláusula 11: No se aplicará el idioma opcional.

3.4. A los efectos de la cláusula 13(a), la autoridad de control competente aplicará lo siguiente:

3.4.1. Cuando el exportador de datos esté establecido en un Estado miembro de la UE, la autoridad de control será la autoridad de control competente para la jurisdicción en la que esté establecido el exportador de datos;

3.4.2. Cuando el exportador de datos esté establecido en el Reino Unido o la transferencia restringida esté sujeta a las leyes y reglamentos de protección de datos del Reino Unido, la autoridad supervisora competente será la Oficina del Comisionado de Información del Reino Unido;

3.4.3. Cuando el exportador de datos esté establecido en Suiza o la transferencia restringida esté sujeta a las leyes y reglamentos de protección de datos de Suiza, el Comisionado Federal de Protección de Datos e Información de Suiza actuará como autoridad supervisora competente; y.

3.4.4. Cuando el exportador de datos no esté establecido en un Estado miembro de la UE, el Reino Unido o Suiza, Pero entra dentro del ámbito de aplicación territorial del Reglamento (UE) 2016/679 De conformidad con su artículo 3, apartado 2, la autoridad de control será la autoridad de control competente para la jurisdicción

en la que esté establecido el representante del exportador de datos, a saber, el Comisario de Protección de Datos de Irlanda.

4. A los efectos de la Cláusula 17 y la Cláusula 18(b), respectivamente, las CCE se regirán por las leyes de la República de Irlanda. Las disputas se resolverán ante los tribunales de Irlanda, excepto que: (i) cuando el exportador de datos esté establecido en Suiza o la Transferencia Restringida esté sujeta a las Leyes y Reglamentos de Protección de Datos de Suiza, los CCE se regirán por las leyes de Suiza y las disputas se resolverán ante los tribunales de Suiza; Y (ii) cuando el exportador de datos esté establecido en el Reino Unido o la Transferencia Restringida esté sujeta a las Leyes y Reglamentos de Protección de Datos del Reino Unido, las CCE se regirán por las leyes del Reino Unido y las disputas se resolverán ante los tribunales del Reino Unido.

5. **Términos adicionales para Suiza**. Cuando el exportador de datos esté establecido en Suiza o la transferencia restringida esté sujeta a las leyes y reglamentos de protección de datos de Suiza: (i) las referencias en las SCC a "Unión Europea", "Unión" o "Estado miembro" se refieren a Suiza; (ii) las referencias al RGPD también incluirán la referencia a las disposiciones equivalentes de la Ley Federal Suiza de Protección de Datos (en su versión modificada o sustituida); Y (iii) las SCC también se aplican a la transferencia de información relacionada con una entidad legal identificada o identificable en la medida en que dicha información esté protegida como Datos Personales bajo las Leyes y Reglamentos de Protección de Datos aplicables de Suiza.

6. **Términos adicionales para el Reino Unido** . Cuando el exportador de datos esté establecido en el Reino Unido o la transferencia restringida esté sujeta a las leyes y reglamentos de protección de datos del Reino Unido:

6.1. Los SCCs se leerán de acuerdo con, y se considerarán enmendados por, las disposiciones de la Parte 2 (Cláusulas Obligatorias) del Apéndice del Reino Unido; y.

6.2. A los efectos de la primera parte, los cuadros 1 y 2 se rellenan con la referencia Anexos A y B (según corresponda) de esta prueba documental, el cuadro 3 se completa con la referencia de la presente prueba documental, Y a los efectos de la Tabla 4, el importador de datos puede finalizar el Apéndice del Reino Unido, tal como se establece en la Sección 19 del Apéndice del Reino Unido.

Anexo A a la prueba 4

APÉNDICE DE LOS SCCS (MÓDULO 2): TRANSFERENCIAS RESTRINGIDAS DE CONTROLADOR A PROCESADOR

ANEXO I

A. LISTA DE PARTES

1. Exportador(s) de datos: [*Identidad y datos de contacto del exportador o exportadores de datos y, en su caso, de su responsable de protección de datos y/o representante en la Unión Europea]*

Nombre	Tal como se proporciona al proveedor bajo el Acuerdo principal
Dirección	Tal como se proporciona al proveedor bajo el Acuerdo principal
Otra información necesaria para identificar la Organización	Tal como se proporciona al proveedor bajo el Acuerdo principal
Nombre de la persona de contacto: Posición: Datos de contacto:	Tal como se proporciona al proveedor bajo el Acuerdo principal
Actividades relacionadas con los datos transferidos en virtud de estos SCC	Como se establece en la cláusula 3 del Anexo anterior
Rol	Controlador

Firma y Fecha del Exportador de Datos: Los SCCs (Módulo 2), junto con este Apéndice y los Anexos del presente documento, se ejecutan como parte del Anexo.

2. **Importador(s) de datos:** [*Identidad y datos de contacto del importador o importadores de datos, incluida cualquier persona de contacto responsable de la protección de datos]*

Nombre	Sophos Limited (para y en nombre de sus filiales de la UE y Suiza)
Dirección	The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido

Otra información necesaria para identificar la Organización	Número de registro 2096520
Nombre de la persona de contacto: Posición: Datos de contacto:	Asesor de privacidad dataprotection@sophos.com
Actividades relacionadas con los datos transferidos en virtud de estos SCC	De acuerdo con el Acuerdo

Firma y Fecha del Importador de Datos: Los SCCs (Módulo 2), junto con este Apéndice y los Anexos del presente documento, se ejecutan como parte del Anexo.

B. DESCRIPCIÓN DE LA TRANSFERENCIA

1.1. Categorías de *sujetos de datos cuyos datos personales se transfieren.*

Como se establece en el documento adjunto 1, Parte A.

1.2 Categorías de *datos personales transferidos.*

Como se establece en el documento adjunto 1, Parte A.

Transferencia de datos sensibles (si procede) y aplicación de restricciones o salvaguardias que tengan plenamente en cuenta la naturaleza de los datos y los riesgos implicados, como, por ejemplo, la limitación estricta del propósito, las restricciones de acceso (incluido el acceso sólo para el personal que haya seguido una formación especializada), manteniendo un registro del acceso a los datos, restricciones para transferencias posteriores o medidas de seguridad adicionales.

Ninguno.

La frecuencia de la transferencia (por ejemplo, si los datos se transfieren de forma continua o en una sola vez).

Continuo.

Naturaleza *de la transformación*

Proporcionar los Servicios contratados por Sophos en virtud y de conformidad con el Acuerdo.

Finalidad(es) de la transferencia de datos y su posterior procesamiento

El Proveedor procesará los Datos Personales del Controlador según sea necesario para realizar los Servicios de conformidad con el Acuerdo y según las instrucciones de Sophos en su uso de los Servicios.

El período durante el cual se conservarán los datos personales o, si no es posible, los criterios utilizados para determinar dicho período

Sujeto a la Sección 10 del Anexo, el Proveedor procesará los Datos Personales durante la duración del Acuerdo, a menos que se acuerde lo contrario por escrito.

Para las transferencias a (sub-) procesadores, especifique también el tema, naturaleza y duración del procesamiento

El Proveedor está autorizado a utilizar los Subprocesadores según lo notificado por el Proveedor a Sophos en el momento de la ejecución del Acuerdo o el Anexo.

C. AUTORIDAD SUPERVISORA COMPETENTE

Como se establece en la sección 3.4del documento adjunto 4.

ANEXO II - MEDIDAS TÉCNICAS Y ORGANIZATIVAS, INCLUIDAS LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA ASETERSE LA SEGURIDAD DE LOS DATOS

Como se establece en el Anexo 2 del Anexo.

ANEXO III – LISTA DE SUBPROCESADORES

No aplicable (las partes han acordado la opción 2 (Autorización general) con respecto a la cláusula 9 (a) de las CCE).