HINWEIS: Dies ist eine maschinell generierte Übersetzung, die lediglich Informationszwecken dient. Diese maschinell generierte Übersetzung entspricht nicht der Qualität menschlicher Übersetzungen und kann Fehler enthalten. Diese Übersetzung wird „WIE SIE IST“ und ohne jegliche Garantie über die Richtigkeit, Vollständigkeit oder Zuverlässigkeit der Übersetzung zur Verfügung gestellt. Im Falle von Widersprüchen zwischen der Originalversion dieses Dokuments in englischer Sprache und übersetzten Versionen hat die englische Version Vorrang.

NACHTRAG ZUR DATENVERARBEITUNG

Revisionsdatum: 20, Januar 2022

Wenn dieser Nachtrag zur Datenverarbeitung („**Nachtrag**“) durch Verweis ausdrücklich in eine Vereinbarung („**Hauptvertrag**“) zwischen Sophos Limited, einem in England und Wales unter der Nummer 2096520 registrierten Unternehmen mit Sitz im The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, UK („**Lieferant**“) und ein Kunde des Lieferanten („**Kunde**“), ist dieser Nachtrag Teil des Hauptvertrags und gilt zwischen dem Lieferanten und dem Kunden.

1. PRÄAMBEL

1.1 Die Parteien haben den Hauptvertrag über die Bereitstellung bestimmter Produkte und/oder Dienstleistungen durch den Lieferanten an den Kunden (gemeinsam „**Produkte**“) abgeschlossen.

1.2 Handelt es sich bei dem Hauptvertrag um einen MSP-Vertrag in ähnlicher Form wie bei dem MSP-Vertrag unter https://www.sophos.com/de-de/legal/sophos-msp-partner-terms-and-conditions.aspx („**MSP-Vertrag**“), ist der Kunde ein Managed Service Provider („**MSP**“). Wenn es sich bei dem Hauptvertrag um einen OEM-Vertrag handelt, nach dem der Kunde berechtigt ist, Produkte von Drittanbietern in Kombination mit den Produkten des Kunden als Teil einer gebündelten Einheit („**OEM-Vereinbarung**“) zu vertreiben, unterlizenzieren oder zur Verfügung zu stellen, ist der Kunde ein Originalgerätehersteller („**OEM**“). Andernfalls ist der Kunde ein Endbenutzer („**Endbenutzer**“).

1.3 Die Bereitstellung der Produkte kann die Erfassung, Verarbeitung und Nutzung von Daten des Verantwortlichen durch den Lieferanten für den Kunden umfassen. Dieser Nachtrag legt die Verpflichtungen der Parteien in Bezug auf diese Datenverarbeitung fest und ergänzt die Bedingungen des Hauptvertrags.

1.4 Der Hauptvertrag, dieser Nachtrag und die im Hauptvertrag und diesem Nachtrag ausdrücklich genannten Dokumente stellen die gesamte Vereinbarung zwischen den Parteien in Bezug auf die vom Lieferanten im Namen des Kunden im Zusammenhang mit dem Hauptvertrag erhobenen, verarbeiteten und verwendeten personenbezogenen Daten dar, Und ersetzt alle früheren Vereinbarungen, Vereinbarungen und Vereinbarungen zwischen den Parteien in Bezug auf diesen Gegenstand.

2. DEFINITIONEN

2.1 In diesem Nachtrag haben die folgenden Begriffe folgende Bedeutung:

„**geltende Datenschutzgesetze**“ bedeutet (i) die EU-Verordnung 2016/679 des Europäischen Parlaments und des Rates über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und den freien Datenverkehr (Datenschutz-Grundverordnung oder „**DSGVO**“); (ii) die e-Privacy-Richtlinie (EU-Richtlinie 2002/58/EG) und (iii) alle anwendbaren nationalen Datenschutzgesetze, einschließlich der Rechtsvorschriften, die gemäß (i) oder (ii) erlassen wurden; in jedem Fall, die von Zeit zu Zeit geändert oder ersetzt werden können.

„**Begünstigter**“ hat die Bedeutung, die ihm im MSP-Abkommen gegeben ist.

„**Controller**“ bedeutet entweder: (A) der Kunde, wenn der Kunde ein Endbenutzer ist; (b) der Begünstigte, wenn der Kunde ein MSP ist; oder (c) der Endkunde, wenn der Kunde ein OEM ist.

„**Daten des Verantwortlichen**“ bezeichnet alle personenbezogenen Daten, für die der Verantwortliche gemäß den geltenden Datenschutzgesetzen der Verantwortliche ist.

„**Endkunde**“ hat die Bedeutung, die ihm im OEM-Vertrag gegeben wird.

„**Europa**“ (und „**europäisch**“) bedeutet (i) die Mitgliedstaaten des Europäischen Wirtschaftsraums („**EWR**“) und (ii) mit sofortiger Wirkung ab dem Datum, ab dem das Unionsrecht für das Vereinigte Königreich und das Vereinigte Königreich nicht mehr gilt.

„EU-Standardvertragsklauseln“ oder „EU-SCCs“ bezeichnet die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, die vom Durchführungsbeschluss (EU) 2021/914 der Europäischen Kommission vom 4. Juni 2021 genehmigt wurde;

„EU-Klauseln vom Controller bis zur Auftragsverarbeiter“ bezeichnet die Module zwei Klauseln zu den EU-SCCs;

„EU-Vertragsverarbeiter-zu-Auftragsverarbeiter-Klauseln“ bezeichnet die Module drei Klauseln zu den EU-SCCs.

„**Hosted Products**“ bezeichnet die in **Anlage 3**aufgeführten Produkte.

„**Verletzung personenbezogener Daten**“ bezeichnet eine Sicherheitsverletzung (mit Ausnahme der Sicherheitsverletzung durch den Kunden oder seine Benutzer), die zu versehentlicher oder rechtswidriger Zerstörung, Verlust, Änderung, unberechtigter Offenlegung oder Zugriff auf Vom Lieferanten gemäß diesem Nachtrag verarbeitete Daten des Verantwortlichen.

„**UK Addendum**“ bezeichnet den Zusatz zu den EU-SCCs, der gegebenenfalls in der Anlage aufgeführt ist.

2.2 In diesem Nachtrag haben die Kleinbuchstaben „**Verantwortlicher**“, „**Auftragsverarbeiter**“, „**betroffene Person**“, „**personenbezogene Daten**“ und „**Verarbeitung**“ (und davon abgeleitete Begriffe) die im geltenden Datenschutzrecht festgelegten Bedeutungen.

3. UMFANG

3.1 Gegenstand und Dauer der Verarbeitung der Daten des Verantwortlichen durch den Lieferanten, einschließlich Art und Zweck der Verarbeitung, der Arten der zu verarbeitenden Daten des Verantwortlichen und der Kategorien der betroffenen Personen, sind wie in beschrieben: (i) dieser Nachtrag; (ii) der Hauptvertrag; (iii) alle Anweisungen in **Anlage 1**; Und (v) die Anweisungen des Kunden, die gemäß Paragraf 4 erteilt wurden.

3.2 Der Kunde ist dafür verantwortlich, (i) sicherzustellen, dass der Verantwortliche über eine rechtmäßige Grundlage für die Verarbeitung von Daten des Verantwortlichen verfügt, die vom Lieferanten in seinem Namen durchgeführt werden, Und (ii) dass der Verantwortliche alle erforderlichen Einwilligungen von betroffenen Personen eingeholt hat, die für die Verarbeitung von Daten des Verantwortlichen durch den Kunden und den Lieferanten erforderlich sein können (einschließlich, aber ohne Einschränkung, in Bezug auf

besondere Kategorien von Daten); Und (iii) dass sie anderweitig den geltenden Datenschutzgesetzen entspricht und sicherstellt, dass ihre Anweisungen an den Lieferanten für die Verarbeitung von Daten des Verantwortlichen in jeder Hinsicht den geltenden Datenschutzgesetzen entsprechen.

3.3 Die übrigen Bestimmungen dieses Nachtrags beschreiben die jeweiligen Verpflichtungen der Parteien in Bezug auf die Daten des Verantwortlichen, für die entweder: (i) der Kunde ist der Verantwortliche und der Lieferant der Auftragsverarbeiter, wenn der Kunde ein Endbenutzer ist; oder (ii) der Kunde ist der Auftragsverarbeiter für einen Drittanbieter-Verantwortlichen und der Lieferant ist der Unterverarbeiter, wenn der Kunde ein MSP oder OEM ist.

4. ANWEISUNGEN DES KUNDEN

4.1 Der Lieferant verarbeitet die Daten des Verantwortlichen in Übereinstimmung mit den dokumentierten Verarbeitungsanweisungen des Kunden, wie ausschließlich in Klausel 3.1 festgelegt, mit Ausnahme von:

(a) Sofern zwischen dem Lieferanten und dem Kunden anderweitig schriftlich vereinbart; oder

(b) Soweit gesetzlich vorgeschrieben, dem der Lieferant unterliegt (in diesem Fall hat der Lieferant den Kunden vor der Verarbeitung über diese gesetzliche Anforderung zu informieren, es sei denn, dieses Gesetz verbietet die Bereitstellung solcher Informationen).

4.2 Sollte der Lieferant Kenntnis davon erhalten, dass die Verarbeitungsanweisungen des Kunden gegen geltende Datenschutzgesetze verstoßen (ohne dem Lieferanten eine Verpflichtung aufzuerlegen, die Einhaltung des Kunden aktiv zu überwachen), wird er den Kunden unverzüglich darüber informieren und die Verarbeitung der Daten des Verantwortlichen aussetzen.

5. PFLICHTEN DES LIEFERANTEN

5.1 Alle Mitarbeiter des Auftragnehmers, die die Daten des Verantwortlichen verarbeiten, müssen in Bezug auf ihre Datenschutz-, Sicherheits- und Vertraulichkeitsverpflichtungen angemessen geschult werden und sind schriftlich zur Wahrung der Vertraulichkeit verpflichtet.

5.2 der Lieferant wird auf eigene Kosten angemessene technische und organisatorische Maßnahmen ergreifen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten und die Daten des Verantwortlichen vor einer Verletzung personenbezogener Daten zu schützen. Bei diesen Maßnahmen werden der Stand der Technik, die Kosten der Umsetzung sowie Art, Umfang, Kontext und Zwecke der Verarbeitung sowie das Risiko einer unterschiedlichen Wahrscheinlichkeit und Schwere der Rechte und Freiheiten natürlicher Personen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten. Die vom Lieferanten ergriffenen Maßnahmen umfassen insbesondere die in **Anlage 2** dieses Nachtrags beschriebenen Maßnahmen. Der Lieferant ist berechtigt, die in **Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen** ohne vorherige schriftliche Zustimmung des Kunden zu ändern oder zu ändern, vorausgesetzt, dass der Lieferant mindestens ein gleichwertiges Schutzniveau besitzt. Auf Verlangen des Kunden wird der Lieferant eine aktualisierte Beschreibung der technischen und organisatorischen Maßnahmen in der in **Anlage 2**dargestellten Form zur Verfügung stellen.

5.3 der Lieferant ist verpflichtet, die in Paragraf 7 festgelegten Anforderungen für die Beauftragung eines Subprozessors zur Verarbeitung von Daten des Controllers zu befolgen.

5.4 der Lieferant hat die in Paragraf 8 genannten Anforderungen zu befolgen, um den Kunden bei der Beantwortung von Anfragen Dritter zu unterstützen, einschließlich aller Anfragen von betroffenen Personen zur Ausübung ihrer Rechte gemäß den geltenden Datenschutzgesetzen.

5.5 nach der Bestätigung des Eintretens einer Verletzung personenbezogener Daten hat der Lieferant den Kunden unverzüglich zu informieren und alle Informationen und die Zusammenarbeit rechtzeitig bereitzustellen, die der Kunde in angemessener Weise für den Kunden (und, falls der Kunde ein MSP oder OEM ist, sein Verantwortlicher) verlangen kann. Zur Erfüllung der Meldepflichten für Datenschutzverletzungen gemäß (und in Übereinstimmung mit den durch das geltende Datenschutzgesetz geforderten Fristen). Der Lieferant hat ferner alle erforderlichen Maßnahmen und Maßnahmen zu ergreifen, um die Auswirkungen der Verletzung personenbezogener Daten zu beheben oder zu mildern, und den Kunden über alle Entwicklungen im Zusammenhang mit der Verletzung personenbezogener Daten auf dem Laufenden zu halten.

5.6 der Lieferant stellt dem Kunden (oder, falls der Kunde ein MSP oder OEM ist, dessen Verantwortlicher) alle angemessenen und rechtzeitigen Hilfestellungen zur Verfügung, die der Kunde (oder, falls zutreffend, der Verantwortliche) zur Durchführung einer Folgenabschätzung für den Datenschutz und ggf. Wenden Sie sich an die zuständige Datenschutzbehörde. Diese Unterstützung ist auf Kosten des Kunden zu leisten.

5.7 der Lieferant hat die Daten des Verantwortlichen innerhalb einer angemessenen Frist nach Beendigung oder Ablauf dieses Nachtrags zu löschen, jeweils wenn und soweit dies nach geltendem europäischem Recht zulässig ist.

5.8 der Lieferant ist verpflichtet, die in Paragraf 6 festgelegten Anforderungen zu befolgen, um dem Kunden (und, wenn der Kunde MSP oder OEM ist, dessen Controller) Informationen bereitzustellen, die erforderlich sind, um die Einhaltung der in diesem Nachtrag festgelegten Verpflichtungen durch den Lieferanten nachzuweisen.

6. AUDIT-RECHTE DES KUNDEN

6.1 der Kunde erkennt an, dass der Lieferant regelmäßig von unabhängigen externen Prüfern gemäß den SSAE 18 SOC 2-Standards geprüft wird. Auf Verlangen hat der Lieferant dem Kunden eine Kopie seines SOC 2-Prüfberichts zu liefern, dessen Berichte den Vertraulichkeitsbestimmungen des Hauptvertrags als vertrauliche Informationen des Lieferanten unterliegen. Der Kunde erkennt an und stimmt zu, dass der externe Prüfer, der diesen Bericht verfasst hat („**Autor**“) keine Verantwortung oder Haftung gegenüber dem Kunden oder den Rechnungsprüfern des Kunden übernimmt, es sei denn, der Kunde schließt mit dem Autor eine separate Sorgfaltspflicht ab. Der Lieferant hat auch auf alle schriftlichen Prüfungsfragen zu antworten, die ihm vom Kunden gestellt wurden, vorausgesetzt, der Kunde wird dieses Recht nicht mehr als einmal pro Jahr ausüben.

7. SUBPROZESSOREN

7.1 der Kunde stimmt den bestehenden Unterauftragsverarbeitern des Lieferanten zum Zeitpunkt dieses Nachtrags zu, die unter https://www.sophos.com/en-us/legal („**Liste der Unterauftragsverarbeiter**“) aufgeführt sind. Der Lieferant verpflichtet sich, die Verarbeitung von Daten des Verantwortlichen ohnevorherige Benachrichtigung des Kunden nicht an weitere Subprozessoren Dritter (jeweils ein „ neuer Subprozessor “) zu übertragen. Der Lieferant ist verpflichtet, die Hinzufügung eines neuen Subprozessors (einschließlich allgemeiner Details zur von ihm ausgeführenden oder durchzuführenden Verarbeitung) vorab zu informieren, die durch die Veröffentlichung von Details zu dieser Hinzufügung in die Liste der Subprozessoren erfolgen kann. Widerspricht der Kunde nicht schriftlich der Bestellung eines neuen Unteraufnehmers durch den Lieferanten (aus angemessenen Gründen im Zusammenhang mit dem Schutz der Daten des Verantwortlichen) innerhalb von 30 Tagen nach der Aufnahme dieses neuen Unteraufnehmers in die Liste der Unteraufnehmer durch den Lieferanten, Der Kunde

erklärt sich damit einverstanden, dass er dem neuen Subprozessor zugestimmt hat. Wenn der Kunde dem Lieferanten einen solchen schriftlichen Einwand vorlegt, hat der Lieferant den Kunden innerhalb von 30 Tagen schriftlich darüber zu informieren, dass entweder: (i) der Lieferant wird den neuen Unterverarbeiter nicht zur Verarbeitung der Daten des Verantwortlichen verwenden oder (ii) der Lieferant ist nicht in der Lage oder nicht bereit, dies zu tun. Wenn die Mitteilung in Absatz (ii) erfolgt, kann der Kunde innerhalb von 30 Tagen nach der Benachrichtigung Diese Ergänzung und den Hauptvertrag hinsichtlich der betroffenen Verarbeitung nach schriftlicher Mitteilung an den Lieferanten zu kündigen, und der Lieferant ist nur für Kunden mit Sitz im Europäischen Wirtschaftsraum und im Vereinigten Königreich verpflichtet, Autorisierung einer anteiligen Rückerstattung oder Gutschrift aller vorausbezahlten Gebühren für den Zeitraum, der nach der Kündigung verbleibt. Wenn jedoch innerhalb dieses Zeitrahmens keine solche Kündigung erfolgt, gilt der Kunde als dem neuen Subprozessor zugestimmt. Der Lieferant verpflichtet sich, neue Unterauftragsverarbeiter mit Datenschutzbedingungen zu versehen, um die Daten des Verantwortlichen gemäß dem in diesem Nachtrag festgelegten Standard zu schützen, und der Lieferant haftet weiterhin uneingeschränkt für jede Verletzung dieses Nachtrags, die durch einen solchen Unterauftragsverarbeiter verursacht wird.

8. ANFRAGEN DRITTER

8.1 der Lieferant leistet dem Kunden (oder, wenn der Kunde MSP oder OEM ist, der Controller) auf Kosten des Kunden alle angemessene und rechtzeitige Unterstützung, um dem Kunden zu ermöglichen, auf Folgendes zu reagieren: (i) jede Aufforderung einer betroffenen Person, eines ihrer Rechte gemäß dem geltenden Datenschutzrecht auszuüben (einschließlich ihrer Rechte auf Zugang, Berichtigung, Widerspruch, Löschung und Datenübertragbarkeit, sofern zutreffend); Und (ii) jede andere Korrespondenz, Anfrage oder Beschwerde, die von einer betroffenen Person, einem Aufsichtsbehörden oder einem anderen Dritten im Zusammenhang mit der Verarbeitung der Daten des Verantwortlichen erhalten wurde. Wenn eine solche Anfrage, Korrespondenz, Anfrage oder Beschwerde direkt an den Lieferanten gestellt wird, hat der Lieferant den Kunden unverzüglich unter Angabe aller Einzelheiten darüber zu informieren.

9. INTERNATIONALE DATENÜBERTRAGUNGEN

9.1 mit bestimmten Produkten kann der Kunde entscheiden, ob die Daten des Verantwortlichen für diese Produkte in Rechenzentren gehostet werden sollen, die sich in (i) dem Europäischen Wirtschaftsraum, (ii) dem Vereinigten Königreich oder (iii) den Vereinigten Staaten von Amerika befinden („**zentraler Speicherort**“). Diese Auswahl erfolgt beim Zeitpunkt der Installation, der Kontoerstellung oder der ersten Verwendung des entsprechenden Produkts. Nach der Auswahl kann der zentrale Speicherort nicht zu einem späteren Zeitpunkt geändert werden.

9.2 der Kunde erkennt an und stimmt zu, dass, unabhängig vom ausgewählten zentralen Speicherort (falls relevant), Daten des Verantwortlichen durch oder in andere Gerichtsbarkeiten (innerhalb und/oder außerhalb des Vereinigten Königreichs und des Europäischen Wirtschaftsraums) exportiert werden dürfen: (i) an Sophos Global Team of Technicians and Engineers for Malware, Security Threat, and false positive Analyse, and Research and Development purposes, (ii) zur Bereitstellung von technischem und Kundensupport, Account Management, Fakturierung und anderen Nebenfunktionen und (iii) wie in der in Klausel 3.1 genannten Dokumentation ausdrücklich beschrieben.

9.3 der Lieferant darf die Daten des Verantwortlichen nicht übermitteln (noch darf er die Verarbeitung der Daten des Verantwortlichen in oder von ihm gestatten) Ein Land außerhalb Europas, es sei denn, die Übertragung erfolgt in ein Land, das nach den geltenden Datenschutzgesetzen als angemessen erachtet wird, oder der Lieferant ergreift die erforderlichen Maßnahmen, um sicherzustellen, dass die Übertragung den geltenden Datenschutzgesetzen entspricht, einschließlich zum Beispiel, jedoch ohne

Einschränkung, Unter Verwendung des EU -SCC (in der von Zeit zu Zeit geänderten Fassung).

9.4 die in Paragraf 9.3 beschriebene Übertragungsbeschränkung gilt auch für die Übermittlung von Daten des Verantwortlichen aus dem Europäischen Wirtschaftsraum in das Vereinigte Königreich, wenn das Vereinigte Königreich nicht mehr dem Unionsrecht unterliegt.

9.5 Wenn Paragraf 9.3 gilt, weil der Lieferant oder ein mit dem Lieferanten verbundenes Unternehmen Daten des Verantwortlichen in einem Land außerhalb des Vereinigten Königreichs oder des EWR verarbeitet, dann in diesem Fall (und nur in dem Umfang, in dem für die Übermittlung von Daten des Verantwortlichen Es sind keine anderen Maßnahmen verfügbar, die nach den geltenden Datenschutzgesetzen anerkannt sind, um solche Übertragungen zuzulassen (wie, ohne Einschränkung, Übertragung an einen Empfänger in einem Land, das nach den geltenden Datenschutzgesetzen als angemessen Schutz für personenbezogene Daten gilt, oder Übertragung an einen Empfänger, der gemäß den geltenden Datenschutzgesetzen eine verbindliche Genehmigung der Unternehmensregeln erhalten hat)) für jede Übertragung von Daten des Verantwortlichen, Die Parteien vereinbaren Folgendes:

(A) für Übertragungen aus dem EWR gelten die Klauseln des EU-Kontrolleurs für Auftragsverarbeiter, und diese SCCs der EU werden hiermit durch Verweis in diesen Nachtrag aufgenommen;

(b) für Übertragungen aus dem Vereinigten Königreich gelten die Klauseln des EU-Kontrolleurs zu Auftragsverarbeitern (und diese EU-SCCs werden hiermit durch Verweis in diesen Nachtrag aufgenommen), vorausgesetzt, dass diese Klauseln des EU-Kontrollers zu Auftragsverarbeitern dem UK-Nachtrag unterliegen.

9.6 Wenn Paragraf 9.3 gilt, weil der Lieferant oder ein Tochterunternehmen des Lieferanten Daten des Verantwortlichen in einem Land außerhalb des Vereinigten Königreichs oder des EWR verarbeitet, dann in diesem Fall (und nur in dem Umfang, in dem für die Übermittlung von Daten des Verantwortlichen Es sind keine anderen Maßnahmen verfügbar, die nach den geltenden Datenschutzgesetzen anerkannt sind, um solche Übertragungen zuzulassen (wie, ohne Einschränkung, Übertragung an einen Empfänger in einem Land, das nach den geltenden Datenschutzgesetzen als angemessen für den Schutz personenbezogener Daten gilt, oder Übertragung an einen Empfänger, der gemäß den geltenden Datenschutzgesetzen eine verbindliche Genehmigung der Unternehmensregeln erhalten hat)), wo (Gemäß Paragraf 3.3(ii)) ist der Kunde der Auftragsverarbeiter für einen Drittanbieter-Controller und der Lieferant der Unterverarbeiter. Die Parteien vereinbaren Folgendes:

(A) für Übertragungen aus dem EWR gelten die EU-Klauseln vom Auftragsverarbeiter zum Auftragsverarbeiter, und diese EU-SCCs werden hiermit durch Verweis in diesen Nachtrag aufgenommen;

(b) für Übertragungen aus dem Vereinigten Königreich gelten die EU-Klauseln vom Auftragsverarbeiter zum Auftragsverarbeiter (und diese EU-SCCs werden hiermit durch

Verweis in diesen Nachtrag aufgenommen), vorausgesetzt, dass diese EU-Klauseln vom Auftragsverarbeiter zum Auftragsverarbeiter dem UK-Nachtrag unterliegen.

9.7 der Anhang zu den SCC der EU ist gemäß Anhang 4 unten auszufüllen.

9.8 für jedes Modul zu den EU-SCCs, falls zutreffend:

(a) Die optionale Docking-Klausel in Klausel 7 gilt nicht;

(b) Es gilt Option 2 gemäß Paragraf 9. Der Datenimporteur benachrichtigt den Datenexporteur 30 Tage im Voraus über beabsichtigte Änderungen (durch Hinzufügen oder Ersetzen) an der Liste der Unterverarbeiter.

(c) In Paragraf 11 gilt die optionale Sprache nicht;

(d) Im Sinne von Paragraf 13(a):

- Hat der Datenexporteur seinen Sitz in einem EU-Mitgliedstaat: Die zuständige Aufsichtsbehörde, die für die Einhaltung der Verordnung (EU) 2016/679 durch den Datenexporteur im Hinblick auf die Datenübertragung zuständig ist, ist die zuständige Aufsichtsbehörde, in der der Datenexporteur seinen Sitz hat und fungiert als zuständige Aufsichtsbehörde.

(e) Im Sinne von Paragraf 17 unterliegen die SCC der EU dem Recht des EU-Mitgliedstaats, in dem der Datenexporteur seinen Sitz hat;

(f) Im Sinne von Ziffer 18 Buchstabe b) werden Streitigkeiten vor den Gerichten des EU-Mitgliedstaats beigelegt, in dem der Datenexporteur ansässig ist.

10. DAUER

10.1 dieser Nachtrag beginnt mit der Unterzeichnung des Hauptvertrags durch beide Parteien (oder dem Datum, an dem der Hauptvertrag in Kraft tritt, falls später) und dauert bis zum früheren Zeitpunkt der: (i) das Auslaufen des Rechts des Kunden auf Nutzung und Erhalt der Produkte, wie im Hauptvertrag oder in Verbindung mit einem zugehörigen Lizenzanspruch angegeben, und (ii) die Beendigung des Hauptvertrags.

11. ANDERE BESTIMMUNGEN

11.1 Änderungen und Ergänzungen dieses Nachtrags bedürfen der Schriftform. Dies gilt auch für Änderungen und Änderungen an dieser Klausel 11.1.

11.2 in keinem Fall übersteigt die Haftung des Lieferanten gegenüber dem Kunden in Verbindung mit Problemen, die aus oder in Verbindung mit diesem Nachtrag entstehen, die im Hauptvertrag festgelegten Haftungsbeschränkungen des Lieferanten. Die im Hauptvertrag festgelegten Haftungsbeschränkungen des Lieferanten gelten in Summe sowohl für den Hauptzusatz als auch für diesen Nachtrag, sodass sowohl für den Hauptvertrag als auch für diesen Nachtrag eine einzige Haftungsbeschränkung gilt.

11.3 dieser Nachtrag unterliegt den Gesetzen von England und Wales und ist in Übereinstimmung mit diesen auszulegen, ohne Rücksicht auf Kollisionsnormen. Soweit dies nach geltendem Recht zulässig ist, sind die Gerichte Englands für die Entscheidung von Streitigkeiten oder Ansprüchen zuständig, die aus, unter oder in Verbindung mit diesem Nachtrag entstehen können.

11.4 im Umfang eines Widerspruchs mit den Bedingungen dieses Nachtrags zur Datenverarbeitung und mit den Bedingungen der von den Parteien einvereinigten SCC haben die Bedingungen der anwendbaren SCC der EU Vorrang.

Anlage 1
Anweisungen Zur Datenverarbeitung

In diesem Anhang 1 wird die Verarbeitung beschrieben, die der Lieferant im Namen des Kunden durchführt.

A) Gegenstand, Art und Zweck der Verarbeitungsvorgänge
Die Daten des Verantwortlichen unterliegen den folgenden grundlegenden Verarbeitungsaktivitäten (bitte angeben):

1. Bereitstellung der vom Kunden im Rahmen und gemäß dem Hauptvertrag erworbenen Produkte
2. Bereitstellung von Account-Management- und Customer Technical Support-Services

Der Lieferant stellt Produkte zur Verfügung, die darauf ausgelegt sind, Sicherheitsbedrohungen innerhalb oder gegen Systeme, Netzwerke, Geräte, Dateien und andere vom Kunden zur Verfügung gestellten Daten zu erkennen, zu verhindern und zu verwalten oder dem Lieferanten dabei zu helfen, Sicherheitsbedrohungen zu erkennen, zu verhindern und zu verwalten. Der Inhalt der in diesen Systemen, Netzwerken, Geräten, Dateien und anderen Daten gespeicherten Informationen wird ausschließlich vom Kunden und nicht vom Lieferanten bestimmt.

(B) Dauer der Verarbeitungsvorgänge:
Die Daten des Verantwortlichen werden für die folgende Dauer verarbeitet (bitte angeben):

Die im Hauptvertrag festgelegte Dauer (oder für die Laufzeit des Hauptvertrags, sofern nicht anders angegeben).

(C) Betroffene
Die Daten des Verantwortlichen betreffen die folgenden Kategorien von betroffenen Personen (bitte angeben):

Zu den betroffenen Personen gehören die Personen, über die dem Lieferanten über die Produkte (oder auf Anweisung des) Kunden oder der Endbenutzer des Kunden‘Daten bereitgestellt werden.

(D) Arten personenbezogener Daten
Die Daten des Verantwortlichen betreffen die folgenden Kategorien von Daten (bitte angeben):

Daten‘Personen, die dem Lieferanten über die Produkte, vom (oder auf Anweisung des) Kunden oder von den Endbenutzern des Kunden zur Verfügung gestellt werden, wie z. B. Kontaktinformationen

(E) Besondere Kategorien von Daten (falls zutreffend)
Die Daten des Rechtsinhabers betreffen die folgenden besonderen Kategorien von Daten (bitte angeben):

Sofern nicht anders angegeben, sind die Produkte des Lieferanten nicht für die Verarbeitung spezieller Datenkategorien ausgelegt.

Anlage 2
Technische und organisatorische Maßnahmen

Bestimmte dieser Maßnahmen können nur für gehostete Produkte relevant oder anwendbar sein.

A) Physische Zugangskontrolle.

- Sophos verfügt über eine Richtlinie zur physischen Zugriffskontrolle;
- Alle Mitarbeiter tragen ID-/Zugangsausweise;
- Die Zugänge zu den Einrichtungen sind durch Zugangsausweise oder Schlüssel geschützt;
- Die Einrichtungen sind unterteilt in (i) öffentliche Zugangsbereiche (wie Empfangsbereiche), (ii) allgemeine Zugangsbereiche für Mitarbeiter und (iii) Bereiche mit eingeschränktem Zugang, die nur von Mitarbeitern mit ausdrücklichem geschäftlichen Bedarf zugänglich sind;
- Zugangsausweise und Schlüssel kontrollieren den Zugang zu eingeschränkten Bereichen innerhalb jeder Einrichtung entsprechend den autorisierten Zugriffsebenen einer Person;
- Zugriffsebenen für Einzelpersonen werden von leitenden Mitarbeitern genehmigt und vierteljährlich überprüft.
- Empfangspersonal und/oder Sicherheitspersonal sind an Eingängen zu größeren Standorten anwesend;
- Einrichtungen sind durch Alarme geschützt;
- Besucher werden vorregistriert und Besucherprotokolle werden gepflegt.

B) System Access Control.

- Sophos verfügt über eine logische Zugriffskontrollrichtlinie;
- Das Netzwerk wird bei jeder Internetverbindung durch Firewalls geschützt;
- Das interne Netzwerk wird je nach Anwendungsempfindlichkeit durch Firewalls segmentiert.
- IDS und andere Threat Erkennung- und Blockierungskontrollen werden auf allen Firewalls ausgeführt;
- Die Filterung des Netzwerkverkehrs basiert auf Regeln, die den Grundsatz des „geringsten Zugriffs“ anwenden;
- Zugriffsrechte werden nur in dem Umfang und für die Dauer gewährt, die für die Ausübung ihrer beruflichen Aufgaben erforderlich ist, und werden vierteljährlich überprüft.
- Der Zugriff auf alle Systeme und Anwendungen wird durch ein sicheres Anmeldeverfahren gesteuert.
- Einzelpersonen verfügen über eindeutige Benutzer-IDs und Kennwörter für ihre eigene Verwendung.
- Passwörter werden auf ihre Stärke getestet und Änderungen werden auf schwache Passwörter durchgesetzt.
- Bildschirme und Sitzungen werden nach einer gewissen Zeit der Inaktivität automatisch gesperrt;
- Sophos-Produkte zum Schutz vor Malware werden standardmäßig installiert.
- An IP-Adressen und -Systemen werden regelmäßig Schwachstellenanalysen durchgeführt.
- Die Systeme werden in einem regelmäßigen Zyklus mit einem Priorisierungssystem zur schnellen Nachverfolgung dringender Patches gepatcht.

C) Datenzugriffskontrolle.

- Sophos verfügt über eine logische Zugriffskontrollrichtlinie;
- Zugriffsrechte werden nur in dem Umfang und für die Dauer gewährt, die für die Ausübung ihrer beruflichen Aufgaben erforderlich ist, und werden vierteljährlich überprüft.
- Der Zugriff auf alle Systeme und Anwendungen wird durch ein sicheres Anmeldeverfahren gesteuert.
- Einzelpersonen verfügen über eindeutige Benutzer-IDs und Kennwörter für ihre eigene Verwendung.
- Passwörter werden auf ihre Stärke getestet und Änderungen werden auf schwache Passwörter durchgesetzt.
- Bildschirme und Sitzungen werden nach einer gewissen Zeit der Inaktivität automatisch gesperrt;
- Laptops werden mit Sophos-Verschlüsselungsprodukten verschlüsselt;
- Die Absender werden angewiesen, die Dateiverschlüsselung vor dem Versenden externer E-Mails in Betracht zu ziehen.

D) Eingangssteuerung.

- Der Zugriff auf alle Systeme und Anwendungen wird durch ein sicheres Anmeldeverfahren gesteuert.
- Einzelpersonen verfügen über eindeutige Benutzer-IDs und Kennwörter für ihre eigene Verwendung.
- Die Sophos Central-Produkte verwenden eine Verschlüsselung auf Übertragungsebene, um Daten während der Übertragung zu schützen;
- Die Kommunikation zwischen der Client-Software und dem Backend-Sophos-System erfolgt über HTTPS, um die Daten während der Übertragung zu sichern, eine Vertrauenskommunikation über Zertifikate und eine Servervalidierung herzustellen.

E) Kontrolle Des Subunternehmers.

- Subunternehmer mit Zugriff auf Daten führen vor der Aufnahme und nach Bedarf ein IT-Sicherheitsvetting-Verfahren durch;
- Verträge enthalten angemessene Vertraulichkeits- und Datenschutzverpflichtungen, die auf den Pflichten des Subunternehmers basieren.

F) Verfügbarkeitskontrolle.

- Sophos schützt seine Betriebsstätten vor Feuer, Überschwemmungen und anderen Umweltgefahren;
- Notstromgeneratoren stehen zur Verfügung, um die Stromversorgung bei Stromausfällen aufrechtzuerhalten;
- Rechenzentren und Serverräume nutzen Klimaregelung und -Überwachung;
- Das Sophos Central-System ist lastausgeglichen und verfügt über ein Failover zwischen drei Standorten, an denen jeweils zwei Instanzen der Software ausgeführt werden, von denen jede den vollständigen Service bereitstellen kann.

G) Segregationskontrolle.

- Sophos unterhält und wendet einen Qualitätskontrollprozess für die Bereitstellung neuer Kundenprodukte an;
- Test- und Produktionsumgebungen sind getrennt;
- Neue Software, Systeme und Entwicklungen werden vor der Freigabe in der Produktionsumgebung getestet.

H) Organisatorische Kontrolle.

- Sophos verfügt über ein dediziertes IT-Sicherheits-Team;
- Der Risk and Compliance Team verwaltet die interne Risikoberichterstattung und -Kontrolle, einschließlich der Berichterstattung über die wichtigsten Risiken für das Management;
- Ein Prozess zur Reaktion auf Vorfälle identifiziert und behebt Risiken und Schwachstellen rechtzeitig;
- Jeder neue Mitarbeiter führt Schulungen zum Datenschutz und zur IT-Sicherheit durch;
- Die IT-Sicherheitsabteilung führt vierteljährliche Kampagnen zum Sicherheitsbewusstsein durch.

Anlage 3
Gehostete Produkte

- Sophos Central
- Sophos Cloud Optix
- Central Device Encryption
- Central Endpoint Protection
- Central Endpoint Intercept X
- Central Endpoint Intercept X Advanced
- Central Mobile Advanced
- Central Mobile Standard
- Central Phish Threat
- Central Intercept X Advanced for Server
- Central Server Protection
- Central Mobile Security
- Central Web Gateway Advanced
- Central Web Gateway Standard
- Central Email Standard
- Central Email Advanced
- Central Wireless Standard
- Alle anderen Sophos-Produkte, die über Sophos Central verwaltet und betrieben werden

Anlage 4

Referenzdaten für EU-STANDARDVERTRAGSKLAUSELN

ANHANG 1 ZU DEN EU-STANDARDVERTRAGSKLAUSELN

A: LISTE DER PARTEIEN

Datenexporteur(e): [*Identität und Kontaktdaten des/der Datenexporteur(e), einschließlich aller für den Datenschutz zuständigen Ansprechpartner]*

Kundenname: Wie dem Lieferanten im Rahmen der Hauptvertrag angegeben

Adresse: wie dem Lieferanten im Rahmen der Hauptvertrag E-Mail-Adresse mitgeteilt:

Name/Position der Kontaktperson: Wie dem Lieferanten im Rahmen des Hauptvertrag angegeben

Aktivitäten, die für die im Rahmen dieser Klauseln übermittelten Daten relevant sind: Wie in Klausel 3 oben beschrieben

Rolle (Controller/Prozessor): Steuerung

Datenimporteur(e): [*Identität und Kontaktdaten des/der Datenimporteur(e) und ggf. seines/ihres Datenschutzbeauftragten und/oder Vertreters in der Europäischen Union]*

Name: Sophos Limited (für und im Namen ihrer Tochtergesellschaften in der EU und der Schweiz)

Adresse: The PENGON, Abingdon Science Park Abingdon, OX14 3YP, UK

Registrierungsnummer: 2096520

Name, Position und Kontaktdaten des Ansprechpartners: dataprotection@sophos.com

Aktivitäten, die für die im Rahmen dieser Klauseln übermittelten Daten relevant sind: Wie in Klausel 3 oben beschrieben.

Rolle (Controller/Prozessor): Prozessor

B. BESCHREIBUNG DER ÜBERTRAGUNG

Kategorien von betroffenen Personen, deren personenbezogene Daten übermittelt werden:

Wie in Abschnitt C, Anlage 1 oben beschrieben

Kategorien der übermittelten personenbezogenen Daten:

Wie in Abschnitt D, Anlage 1 oben beschrieben.

Vertrauliche Daten, die (falls zutreffend) übertragen und Beschränkungen oder Garantien angewendet werden, die die Art der Daten und die damit verbundenen Risiken vollständig berücksichtigen, wie z. B. strenge Zweckbeschränkungen, Zugriffsbeschränkungen (einschließlich des Zugriffs nur für Mitarbeiter, die spezielle Schulungen absolviert haben), eine Aufzeichnung des Zugriffs auf die Daten führen, Beschränkungen für Weiterüberweisungen oder zusätzliche Sicherheitsmaßnahmen:

Wie in Abschnitt E, Anlage 1 oben beschrieben.

Die Häufigkeit der Übertragung (z. B. ob die Daten einmal oder kontinuierlich übertragen werden).

Kontinuierlich

Art der Verarbeitung

Wie in Abschnitt A, Anlage 1 oben beschrieben.

Zweck(e) der Datenübermittlung und Weiterverarbeitung

Wie in Abschnitt A, Anlage 1 oben beschrieben.

Die Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien, die zur Bestimmung dieser Dauer verwendet werden

Für die Dauer der Vertragslaufzeit.

Geben Sie bei Übertragungen an (Sub-) Auftragsverarbeiter auch den Gegenstand, die Art und die Dauer der Verarbeitung an

Wie in Klausel 3 oben beschrieben.

ZUSTÄNDIGE AUFSICHTSBEHÖRDE

SIEHE ZIFFER 9.8 OBEN

ANHANG II – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH TECHNISCHER UND ORGANISATORISCHER MASSNAHMEN ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN[1]

Die Maßnahmen sind in der obigen Anlage 2 dargelegt.

ANHANG III – LISTE DER UNTERVERARBEITER[2]

Nicht erforderlich als Klausel 9(a) wurde Option 1 **nicht** ausgewählt.

[1] Anhang II muss für alle Module mit Ausnahme VON MODUL 4ausgefüllt werden.
[2] Anhang III gilt nur für MODUL ZWEI (Transfer Controller to Processor) und MODUL DREI (Transfer Processor to Processor), wenn Klausel 9(a), Option 1) ausgewählt wurde.