注意：這是機器生成的翻譯，僅為方便起見而提供。這種機器生成的翻譯與人工翻譯的質量不匹配，可能存在錯誤。本翻譯「按原樣」提供，不保證翻譯的準確性、完整性或可靠性。 如果本協定的英語版本與任何翻譯版本之間存在任何不一致之處，請以英語版本為準。

數據處理附錄

修訂日期：18，2022 年 12 月

如果此數據處理附錄（“附錄”）明確納入 Sophos Limited（一家在英格蘭和威爾士註冊的公司，編號爲 2096520）的主要協議（定義見第 2 條），註冊辦事處設在五角大樓、Abingdon 科學園、Abingdon、Oxfordshire、OX14 3YP、英國（“供應商”）和供應商客戶（“客戶”），此附錄構成主要協議的一部分，並且在供應商和客戶之間有效。

本附錄中使用的大寫術語定義如下文第 2 條所述。如有要求、我們可能會以其他語言提供本附錄的複本。若發生衝突、應以英文版的附錄為規範。

1. 序言

1.1. 雙方已就供應商向客戶提供某些產品和 / 或服務（統稱“產品”）達成主要協議。

1.2. 如果主協議是與位於 https://www.sophos.com/en-us/legal/sophos-msp-partner-terms-and-conditions （“MSP 協議”）的 MSP 協議類似的 MSP 協議，則客戶是託管服務提供商（“MSP”）。如果主協議是 OEM 協議，根據該協議，客戶有權與客戶的產品一起作爲捆綁設備的一部分（“ OEM 協議”）分發、從屬許可或向第三方供應商產品提供，則客戶是原始設備製造商（“ OEM ”）。否則，客戶是最終用戶（“最終用戶”）。

1.3. 提供產品可能包括供應商代表客戶收集、使用及其他處理控制器個人資料。本增編規定了當事各方在這種處理方面的義務，並補充了主要協議的條款和條件。

1.4. 儘管協議或本附錄有任何其他條款，雙方同意控制器個人數據不應包括聯繫信息、付款或帳單信息，或有關業務聯繫人和客戶管理員的其他個人數據，包括姓名、電子郵件地址和聯繫信息，哪些供應商代表其自己收集和處理，以便管理其客戶關係、與當前、前客戶和潛在客戶及業務合作伙伴進行通信，以及管理其業務關係（“CRM 數據”）。

1.4.1. 供應商是 CRM 數據的控制器，將根據其根據適用的數據保護法律 和 供應商組隱私聲明所承擔的義務處理 CRM 數據。

1.4.2. 除第節 1.4.1 外，供應商根據本附錄承擔的義務不適用於 CRM 數據。

1.5. 主要協議、本附錄以及主要協議和本附錄中明確提及的文檔應構成雙方就供應商代表客戶就主要協議收集、處理和使用的個人數據達成的完整協議， 並應取代雙方先前就該主題事項達成的所有協議、安排和諒解。

2. 定義

2.1. 在本附錄中，下列詞語具有下列涵義：

“適用的數據保護法律”是指在適用範圍內：(a) 歐盟議會和理事會關於保護自然人處理個人數據和自由移動此類數據的條例 2016/679 （一般數據保護條例或 "GDPR" ）；(b) 電子隱私指令（歐盟指令 2002/58/EC ）；及 (c) 任何及所有適用的國家數據保護法規，包括根據或依據 (a) 或 (b) 制定的法律；在每種情況下，均可不時予以修訂或取代。

“受益人”在 MSP 協議中有其含義。

“CPA”是指經《2020 年加利福尼亞隱私權法》修訂的《加利福尼亞消費者隱私法》，該法在 Cal.錢法規 § § 1798.100 - 1798.199.100 及其頒佈的《加利福尼亞消費者隱私法條例》，加利福尼亞州代碼註冊。tit.11, div. 6, ch. 1、經修正的每一項；

“條款”具有《管制條例》所賦予的涵義。

“控制器”意指：(a) 客戶（如果客戶是最終用戶）；(b) 受益人（如果客戶是 MSP ）；或 (c) 最終客戶（如果客戶是 OEM ）。

“控制人個人數據”是指供應商根據服務代表控制人處理的個人數據。

“控制器至處理器條款”是指對 SCC 的模塊二條款。“CRM 數據”是指聯繫信息、付款或開單信息，或有關業務聯繫人和客戶管理員的其他個人數據，包括姓名、電子郵件地址和聯繫信息，哪些供應商會自行收集和處理、以管理其客戶關係、與目前、前客戶和潛在客戶及業務合作夥伴溝通、並以其他方式管理其業務關係。

“數據主題”是指 Sophos 個人數據與之相關的個人。

“數據主題請求”是指數據主體根據適用的數據保護法律行使權利的任何請求，包括其訪問、刪除和更正權利。

"歐洲經濟區"是指歐洲經濟區，包括(a)歐洲經濟區("歐洲經濟區")的成員國和(b)聯合王國。

“最終客戶”在 OEM 協議中具有其含義。

“歐洲”(和“歐洲”)指(a)歐洲經濟區(“歐洲經濟區”)的成員國和(b)聯合王國。

“託管 產品”是 指圖 3 中列出的產品。

“ICO”是指在聯合王國設立的新聞專員辦事處

「主要合約」係統指書面合約，包括及證明、增編及修訂合約，據此，供應商向客戶提供若干服務。

“個人數據”是指任何可識別、可用於識別或以其他方式與特定個人或家庭相關或合理關聯的信息，以及根據適用的數據保護法律和規章定義爲“個人數據”、“個人信息”或同等術語的任何信息。

「個人資料外洩」意指違反安全性(客戶或其使用者所造成者除外)，導致意外或非法的銷毀、遺失、修改、未經授權的揭露或存取，供應商根據本附錄處理的控制器個人資料。

“處理器”是指根據財務主任的指示代表個人數據處理的個人或實體，包括根據 CPA 作爲“服務提供商”的任何實體。

「限制轉移」是指客戶將控制器個人資料移轉給供應商、若無適用的標準合約條款及適用的英國附錄、適用的資料保護法將禁止此類轉移。

“敏感數據”是指“特殊類別的個人數據”、“敏感個人數據”、“敏感數據”以及根據適用的數據保護法律定義的等效術語。

“服務”是指供應商根據主要協議提供的所有產品和/或服務。

"標準合同條款"或"標準合同條款"是指根據歐洲議會條例 2016/679 和歐洲委員會執行 2021/914 號決定所批准的理事會將個人數據轉移到第三國的標準合同條款。

“子處理器”是指由供應商指定或代表供應商指定的處理控制器個人數據的任何個人或實體（不包括供應商的任何員工）或實體。

「監管機關」係指有關適用之資料保護法律與法規的主管監管機關、包括適用之 GDPR 所定義之監管機關。

「英國增編」指由 ICO 不時 修訂或取代之歐盟委員會標準合約條款之國際資料傳輸增編，該增編由英國相關資料保護法例所規定之主管監管機關取代

2.2. 在本附錄中，小寫的術語 "控制器" 、" 處理器" 、" 數據主題" 、 "個人數據" 和 "處理" （及其衍生性產品）應具有適用的數據保護法中所賦予的含義。

3. 範圍

3.1. 供應商處理主計長個人資料的主題事項和期限、包括處理的性質和目的、要處理的主計長個人資料類型、以及資料主題的類別、應如下列所述：(a)本附錄；(b)主要協議；(c)附件 1（數據處理說明）中的任何指示；(d)客戶按照下文第 4 條發出的指示。

3.2. 客戶有責任確保（a）控制器有合法的基礎來處理供應商代表客戶執行的控制器個人數據，(b)財務總監已取得客戶及供應商處理財務總監個人資料所需之資料當事人之所有必要同意

書（包括但不限於敏感資料）；以及（c）該資訊符合並將確保其指示供應商處理控制器個人資料、在所有方面均符合適用的資料保護法律。

3.3. 雙方同意供應商為控制器個人資料的處理器或子處理器、且客戶為（a）客戶為終端使用者的控制器、或（b）客戶為 MSP 或 OEM 的處理器（（適用於第三方控制器）。

4. 客戶指示

4.1. 客戶指示供應商根據合理需要處理控制器個人資料、以提供及執行服務、以及本合約及主要合約中的其他規定。供應商應依照客戶的書面處理指示處理控制器個人資料、如本文件所述、除非（a）供應商與客戶另有書面協議；或（b）供應商受其管轄的法律規定（在此情況下、供應商應在處理前告知客戶該法律規定、除非該法律禁止提供此類資訊）。

4.2. 如果供應商得知客戶的處理指示違反適用的資料保護法律（不強制供應商主動監控客戶的合規性）、供應商會立即通知客戶相同的資訊、並暫停處理控制器個人資料。

4.3. 在不限制禁止的情況下，在加利福尼亞消費者隱私法（“**CPA**”）適用於控制器個人數據的範圍內，供應商 還同意：

4.3.1. 供應商不得使用、揭露或以其他方式處理控制器個人資料、除非是為了執行服務的特定目的、且必須遵守本附錄與主要合約的條款、並遵守適用法律的其他規定。儘管有上述規定：

a. 供應商可委聘子處理器處理控制器個人資料、但須遵守第 7 節的條款；

b. 供應商不得在 客戶與供應商之間的直接業務關係之外處理 控制器個人數據，或爲供應商自身的商業目的處理控制器個人數據；儘管有上述規定、雙方同意、在 CCPA 適用的範圍內、供應商僅會針對主要協議和本附錄中所述的特定業務目的、或為 CCPA 法規明確授權的其他目的、處理控制器個人資料。

c. 供應商不會「分享」或「賣出」（因為這些條款是根據 CPA 定義）任何控制器個人資料；

d. 供應商會（並會促使每個分處理器）遵守 其根據 CPA 所承擔的義務、並會提供與 CPA 所要求的相同等級的隱私保護；以及

e. 如果供應商認為無法遵守本附錄或適用的資料保護法律的條款、供應商會立即通知客戶、 並授予客戶採取合理且適當步驟的權利 、 以確保控制器個人資料的處理方式符合控制器根據 CCPA 所承擔的義務。

f. 供應商不會在主協議到期或終止時保留控制器個人數據，除非第節中規定 8；

5. 供應商的責任

5.1. 處理主計長個人資料的所有供應商人員、應接受充分的資料保護、安全與保密義務訓練、並應遵守書面或法定義務以維護機密性。

5.2. 供應商將實施適當的技術和組織措施，以確保安全級別適合風險，並保護控制器個人數據免遭個人數據泄露。這些措施將考慮到最新的情況、執行的費用以及性質、範圍、 處理的背景和目的以及自然人的權利和自由的可能性和嚴重性各不相同的風險，以確保對風險適當的安全程度。供應商採取的措施尤其應包括 本增編附件 2 所述措施。供應商可在 未 事先取得客戶書面同意的情況下、變更或修改附件 2 所述的技術和組織措施、但供應商必須維持至少同等程度的保護。應客戶要求，供應商將按 附件 2 所示的形式提供技術和組織措施的最新說明。

5.3. 供應商應遵循以下第 7 條所規定的要求、委聘任何子處理器來處理控制器個人資料。

5.4. 供應商應遵循下文第 8 條所述的要求、協助客戶回應第三方的查詢、包括資料當事人根據適用的資料保護法律行使其權利的任何要求。

5.5. 在確認發生任何個人資料外洩事件時、供應商應立即通知客戶、並應提供客戶合理要求的所有及時資訊與合作、以利客戶（若客戶為 MSP 或 OEM 、則為其控制人） 根據適用的資料保護法、履行其資料外洩報告義務（並依照規定的時限）。供應商應進一步採取合理必要的措施和行動、以補救或減輕個人資料外洩的影響、並應隨時告知客戶與個人資料外洩有關的發展。

5.6. 供應商應以客戶（或在適用情況下、控制器）的合理且及時的協助、提供客戶（或客戶為 MSP 或 OEM） 可能需要進行數據保護影響評估或其他評估，這些評估需要由適用的數據保護法律進行，必要時還需要諮詢相關的數據保護機構。此類協助應由客戶自費提供。

5.7. 除非適用法律另有規定，否則供應商應在本附錄終止或到期後的合理期間內刪除財務總監的個人數據，除非適用法律禁止。應客戶要求、供應商將向客戶確認此類控制人個人資料已根據本附錄刪除。如果適用法律要求供應商保留任何控制器個人資料、供應商應採取步驟、確保控制器個人資料在維護期間持續保密與安全。

6. 客戶的審覈權限

6.1. 客戶確認供應商係由獨立第三方稽核員定期根據 SSAE 18 SOC 2 標準進行稽核。供應商應在合理的要求下，向客戶提供一份 SOC 2 審計報告，該報告應遵守主要協議的保密規定，作爲供應商的機密信息。供應商也應回應客戶提交給客戶的合理書面稽核問題、但客戶不得每年行使此項權利超過一次。

6.2. 如果客戶合理認為，根據第 6.1 條提供的材料不足以證明供應商遵守本附錄的規定，客戶可以書面要求並遵守本附錄第 6.2 條(a)至(d)款的規定，該供應商向客戶提供所有合理必要的

信息，以證明遵守本附錄中規定的義務（包括適用範圍內的標準合同條款），並允許客戶或客戶的獨立人員進行審計（包括檢查）並對審計做出貢獻，非本附錄所涵蓋之處理活動供應商競爭對手的第三方稽核員。

a. 在根據本條款 6.2 要求審查或稽核之前、客戶將考量第 6.1 條所述的相關供應商第三方認證和稽核；

b. 客戶應至少提前 60 天向處理器發出合理通知，要求根據本條款 6.2 進行審計或檢查，並將採取（並確保其每位審計員採取）合理措施以避免和防止任何損害或傷害，並儘量減少此種審計或檢查所造成的任何干擾；

c. 除非監管機關或適用的資料保護法有要求、否則每年最多不會進行一次稽核或檢查；以及

d. 客戶應承擔任何此類審計的全部費用，並應向供應商償還供應商根據此類審計所產生的合理費用和開支，包括供應商、其關聯機構或其子處理器按供應商當時的專業服務費率進行任何此類審計或檢查所花費的任何時間，應客戶要求提供。

7. 子處理器

7.1. 客戶同意在本附錄之日使用供應商現有的子處理器，這些子處理器列於 https://www.sophos.com/en-us/legal（“子處理器列表”）以及供應商關聯機構。客戶明確同意供應商同意接受額外的第三方子處理器（每個“新子處理器”），但須遵守本條款 7 中規定的條款。供應商會在新增任何新的子處理器前三十（30）天通知客戶、此通知可透過張貼此類新增至子處理器清單的詳細資料而發出。

7.2. 如果客戶在供應商將新的子處理器添加到子處理器列表的 30 天內不反對供應商指定新的子處理器（基於與控制器個人數據保護有關的合理理由），客戶同意將被視爲已同意該新子處理器。如果客戶向供應商提出此類書面異議，供應商將在 30 天內以書面形式通知客戶：（a）供應商不會使用新的子處理器來處理控制器個人資料；或（b）供應商無法或不願意這樣做。如發出第 (b) 段所述的通知，客戶可在該通知發出後 30 天內，選擇在書面通知供應商和供應商時終止本附錄和受影響處理的主要協議，僅適用於位於歐洲經濟區和英國的客戶，授權依比例退款或將終止後剩餘期間的任何預付費用入帳。然而、如果在該期間內未提供此類終止通知、則客戶將被視為已同意新的子處理器。供應商將根據本附錄的規定、對控制器個人資料實施同等保護的新子處理器實施資料保護條款。供應商將對每個子處理器的義務的履行負全部責任。

8. 第三方的詢問

8.1. 供應商應將其從資料當事人、主管機關或其他第三方收到的任何與控制人個人資料處理有關的隱私要求、信函、詢問或投訴通知客戶、並提供該資料當事人的完整詳細資料、但不得直接回應資料當事人、但法律另有規定者除外。

8.2. 在必要的範圍內，供應商將向客戶（或者，如果客戶是 MSP 或 OEM，則爲控制器）提供合理及時的幫助，並由客戶承擔費用，使客戶（或者如果客戶是 MSP 或 OEM，則爲控制器）能夠對以下事項作出響應：(a)資料當事人根據適用的資料保護法行使其權利的要求(包括在適用的情況下，其存取權、更正權、反對權、刪除權和資料可攜性，AS 和(b)從監管機構或其他第三方收到的與控制器個人數據處理有關的請求。

9. 國際數據傳輸

9.1. 某些產品可讓客戶選擇將此類產品的控制器個人資料存放在何處、包括可能位於資料來源所在轄區以外的資料中心。這些地點可包括(a)歐洲經濟區、(b)聯合王國、(c)美利堅合衆國；或主要協定所規定的另一個地點("中央儲存位置")。此選擇在產品安裝、帳戶創建或首次使用相關產品時進行。選擇後，中心存儲位置將無法在以後更改。

9.2. 客戶繼承者承認並明確同意（無論所選的中央儲存位置（如果相關））限制轉讓，但須遵守本條款 9 中規定的義務。

9.3. 關於任何限制轉讓：

9.3.1. SCC 和英國增編明確納入本附錄、並構成本增編的一部分；

9.3.2. 在遵守 9.3.3 本協議第 4 節 和第 4 部分的前提下，客戶和供應商特此簽訂並同意：（i）SCC、適用於將控制器個人資料限制轉讓給供應商的範圍；及(ii)英國增編，適用於及修訂及補充受英國資料保護法及規例規限的管制人個人資料的任何限制轉讓；及

9.3.3. 《管制條例》第 2 單元應適用，但須符合本文件附件 4 的條款。

9.4. SCC 的附錄應按下文附件 4 所列方式填寫。

10. 持續時間

10.1. 本增編自(a)雙方執行主要協議或(b)主要協議生效之日（如較晚）起生效，並持續至以下日期之前：(i) 客戶使用和接收產品的權利到期，如主協議或任何相關的許可證權利中所述；以及 (ii) 主協議的終止。

11. 其他法規

11.1. 對本增編的修改和修正需要書面形式。這也適用於對本條款 11.1 的更改和修改 11.1。

11.2. 在任何情況下、供應商對於因本附錄所引起或與本附錄相關的任何問題、對客戶的責任、均不得超過供應商在主要合約中所規定的責任限制。供應商對主要協議中規定的責任的限制應在主要協議和本附錄中綜合適用，因此對責任制度的單一限制應適用於主要協議和本附錄。

11.3. 本附錄（不包括 SCC）應受英格蘭和威爾斯法律管轄並依其解釋、而不考慮法律衝突原則。在適用法律允許的範圍內，英格蘭法院具有專屬管轄權，可決定因本附錄、根據本附錄或與本附錄相關的任何爭議或索賠。

11.4. 在與本數據處理增補件條款和當事方訂立的任何 SCC 條款發生衝突的情況下，適用的 SCC 條款（包括其任何附件）應優先。

12. 法律變革

12.1. 若因變更適用的資料保護法而需要對本附錄進行任何修改、則任一方均可向該法律變更的另一方提供書面通知。各方將真誠地討論和談判本增編的任何必要改動，以處理這些改動。雙方不會不合理地拒絕同意或同意根據本節 12 或其他方式修改本附錄。

12.2. 若標準合約條款或英國附錄以新版本（「新條款」）取代、更新或取代、客戶同意供應商可在事先書面通知客戶後、視需要更新本附錄、以納入新條款、作為先前標準合約條款或英國附錄之修訂或取代。

附件 1.

處理說明

此圖 1 描述供應商將代表客戶執行的處理。

(a) 處理作業的主題、性質和目的

主計長個人資料將受下列基本處理活動規範（請具體說明）：

- 提供客戶根據主要協議並根據主要協議購買的產品
- 提供客戶管理和客戶技術支持服務

供應商提供的產品旨在偵測、預防及管理或協助供應商偵測、預防及管理系統、網路、裝置、檔案及客戶提供的其他資料內或其所造成的安全威脅。這些系統、網路、裝置、檔案及其他資料中所持有之任何資訊的內容僅由客戶決定、而非由供應商決定。

(b) 處理作業的持續時間：

控制器個人數據將在以下時間內處理（請具體說明）：

主要協議中指定的持續時間（或主要協議期限，如果未另行指定）。

(c) 數據主題

控制器數據涉及以下類別的數據（請具體說明）：

- 客戶的人員和最終用戶
- 代表客戶處理其個人數據的其他與 Sophos 產品相關的數據主題

(d) 個人資料的類型

主計長個人資料涉及下列資料類別（請說明）：

- 用戶名和其他標識符
- 網絡和網絡活動信息
- 與 Sophos 產品相關的其他信息可能被傳輸或處理

(e) 特殊類別的數據 (如適用)

主計長個人資料涉及下列特殊類別的資料（請說明）：

除非另有說明，否則供應商的產品並非設計用於處理特殊類別的數據。

SOPHOS

附件 2.

技術和組織措施

這些措施中的某些可能僅適用於託管產品。

1. 物理訪問控制。
   (a) Sophos 有實際的出入管制政策；
   (b)所有工作人員均攜帶身份證/出入證；
   (c)進入設施的入口受到出入證或鑰匙的保護；
   (d)設施分爲：㈠公共出入區（如接待區）；㈡一般工作人員出入區；和㈢只有具有明確業務需要的人員才能進入的限制出入區；
   (e)出入證和鑰匙根據個人的授權進入級別控制對每個設施內限制區的出入；
   (f)個人的進入水平由高級工作人員覈准，每季度覈實；
   (g)接待和/或保安人員在較大地點的入口處；
   (h)設施受到警報保護；
   (i)訪客已預先登記，訪客日誌保持不變。

2. 系統訪問控制。
   (a) Sophos 具有邏輯訪問控制策略；
   (b)網絡在每個 Internet 連接上受防火牆保護；
   (c)內部網絡根據應用程序敏感度由防火牆分割；
   (d) IDS 以及在所有防火牆上運行的其他威脅檢測和阻止控制；
   (e)過濾網絡流量是根據適用"最少訪問"原則的規則；
   (f)只有在必要的範圍內和期限內授權人員才能行使其工作職責，並每季度審查一次；
   (g)對所有系統和應用程序的訪問由安全登錄過程控制；
   (h)個人有唯一的用戶 ID 和密碼供自己使用；
   (i)密碼經過強度測試，並強制更改爲弱密碼；
   (j)在一段時間不活動後屏幕和會話自動鎖定；
   (k) Sophos 惡意軟件保護產品作爲標準安裝；
   (l)定期對 IP 地址和系統進行漏洞掃描；
   (m)系統定期進行修補，並使用優先級系統快速跟蹤緊急修補程序。

3. 數據訪問控制。
   (a) Sophos 具有邏輯訪問控制策略；
   (b)只有在必要的範圍和期限內授權人員才能執行其工作角色，並每季度審查一次訪問權限；
   (c)對所有系統和應用程序的訪問權限由安全登錄過程控制；
   (d)個人有自己使用的唯一用戶 ID 和密碼；
   (e)對密碼進行強度測試，對弱密碼進行更改；

(f)在一段時間不活動後屏幕和會話自動鎖定；

(g)使用 Sophos 加密產品對筆記本電腦進行加密；

(h)寄件者在傳送任何外部電子郵件之前，必須考慮檔案加密。

4. 輸入控制。

(a)對所有系統和應用程序的訪問由安全的登錄過程控制；

(b)個人擁有唯一的用戶 ID 和密碼供自己使用；

(c) Sophos Central 產品使用傳輸層加密來保護傳輸中的數據；

(d)通過 HTTPS 執行客戶端軟件與後端 Sophos 系統之間的通信，以保護傳輸中的數據，通過證書和服務器驗證建立信任通信。

5. 分包商控制。

(a)有權訪問數據的分包商在啓動前和以後的要求下，都要進行 IT 安全審覈程序；

(b)合同根據分包商的責任規定適當的保密性和數據保護義務。

6. 可用性控制。

(a) Sophos 保護其房舍免受火災、水災和其他環境危害；

(b)備用發電機可在停電時維持供電；

(c)數據中心和服務器室使用氣候控制和監測；

(d) Sophos Central 系統負載平衡，在三個站點之間進行故障切換，每個站點運行兩個軟件實例，其中任何一個都能提供完整服務。

7. 隔離控制。

(a) Sophos 維護並應用了部署新客戶產品的質量控制流程；

(b)測試和生產環境是分開的；

(c)在發佈到生產環境之前對新軟件、系統和開發進行了測試。

8. 組織控制。

(a) Sophos 擁有一個專門的 IT 安全小組；

(b)風險和合規性小組管理內部風險報告和控制，包括報告對管理的關鍵風險；

(c)事件響應流程及時識別和補救風險和漏洞；

(d)每個新員工都進行數據保護和 IT 安全培訓；

(e) IT 安全部門每季度進行一次安全意識活動。

附件 3.

託管產品

(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) 通過 Sophos Central 管理和操作的任何其他 Sophos 產品

附件 **4.**

限制轉讓的其他條款

本附件包括客戶或代表客戶根據附錄向供應商進行的限制轉讓適用的附加條款，以及完成適用SCC附錄（附件I-III）所需的信息。

雙方同意本增編，即同意並據此在所有相關部分執行SCC，但須遵守 9 增編第節 和本附件的條款。

1. 本附件或附錄所用但未定義的詞彙，須具有《證券及交易管理委員會》及《英國增編》所賦予的涵義（視適用情況而定）。

2. 《證券及交易管理委員會條例》第2條適用，但須受本附件的條款規限，而《證券及交易管理委員會條例》的附錄須參照本文件附件A填寫。

3. 對於SCC（模塊2）：

3.1. 第7條：任擇的對接條款不適用；

3.2. 條例草案第9(a)條：備選案文2（一般授權）應適用、且資料進口商應在任何預期變更之前至少30天以書面通知資料出口商。

3.3. 第11條：任擇語文不適用。

3.4. 就第13(a)條而言，主管監督機關適用下列規定：

3.4.1. 如果在歐盟成員國建立數據出口國，監督當局將是建立數據出口國管轄區的主管監督機構；

3.4.2. 如果在英國設立數據出口者或限制轉讓受聯合王國的數據保護法律和條例的約束，主管監督機構應爲聯合王國信息專員辦事處；

3.4.3. 如果資料出口商在瑞士設立、或是限制轉移受瑞士資料保護法律與法規的規範、則瑞士聯邦資料保護與資訊專員應擔任主管監督機關；以及

3.4.4. 如果數據出口國不是在歐盟成員國、聯合王國或瑞士建立的，但是，根據第3(2)條，屬於條例 2016/679 的適用範圍，監督當局將是建立數據出口者代表的管轄區的主管監督機構，即愛爾蘭數據保護專員。

4. 就第17條和第18(b)條而言，SCC應受愛爾蘭共和國法律管轄，爭端將由愛爾蘭法院解決，但下列情況除外：(i)如果數據出口者在瑞士設立或限制轉讓受瑞士數據保護法律和條例的約束，SCC應受瑞士法律的管轄，爭端將在瑞士法院解決；(ii)倘資料輸出者在英國設立或限制轉讓受英國資料保護法例及規例規管，則SCC須受英國法律管轄，而爭議將於英國法院解決。

5. **瑞士的附加條款**。如果資料匯出者是在瑞士設立、或是限制傳輸受瑞士資料保護法律與法規的規範：(i) SCC中提到"歐盟"、"聯盟"或"成員國"，即瑞士；(ii)提到GDPR，還應包括提到瑞士聯邦數據保護法（經修訂或取代）的同等條款；及(iii)倘

有關資料根據瑞士適用之資料保護法例及規例受個人資料保護，則SCC亦適用於與已識別或可識別之法律實體有關之資料傳輸。

6. **聯合王國的附加條款**。若資料出口商在英國成立或限制轉讓受英國資料保護法律與法規的規範：

6.1. 《證券及交易管理委員會條例》須按照英國增編第2部(必備條款)的條文而理解，並當作修訂；及

6.2. 就第一部分而言，表1及表2已填妥，並附有本附件A及B (如適用)之參考資料，表3乃參照本附件所載資料而填寫，就表4而言、資料進口商可依照英國附錄第19節的規定、終止英國附錄。

附件 A 至附件 4

SCC 附錄（模塊 2）：控制器到處理器的傳輸受限

附件一

A. 締約方名單

1.資料匯出器：[*數據出口者的身份和聯繫細節，以及其數據保護幹事和/或歐洲聯盟代表的身份和聯繫詳情*]

名稱	根據主要協議提供給供應商
地址	根據主要協議提供給供應商
查明本組織所需的其他資料	根據主要協議提供給供應商
聯繫人姓名： 職位： 聯絡詳情：	根據主要協議提供給供應商
與根據這些 SCC 轉移的數據有關的活動	如上文增編第 3 條所載
角色	控制器

數據導出器簽名和日期：SCC（單元 2）連同本附錄及本附錄附件一併作爲附錄的一部分執行。

2.資料匯入程式：[*數據導入程序的身份和聯繫人詳細信息，包括負責數據保護的任何聯繫人。*]

名稱	Sophos Limited （代表其歐盟及瑞士附屬公司）
地址	The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
查明本組織所需的其他資料	註冊號碼 2096520
聯繫人姓名： 職位：	隱私權顧問 dataprotection@sophos.com

聯絡詳情：	
與根據這些 SCC 轉移的數據有關的活動	根據協議

數據導入器簽名和日期：SCC（單元 2）連同本附錄及本附錄附件一併作爲附錄的一部分執行。

B. 轉讓說明

1.1. *傳輸個人數據的數據主題*的類別。

如附件 1 A 部分所述

1.2 傳輸*的個人資料類別。*

如附件 1 A 部分所述

敏感數據的傳輸（如果適用）和應用的限制或保障措施充分考慮到數據的性質和所涉及的風險，例如嚴格的目的限制、訪問限制（包括僅對經過專門培訓的工作人員的訪問），保存對數據的訪問記錄，對轉接或其他安全措施的限制。

無。

傳輸頻率（例如，數據是一次性還是連續性傳輸）。

連續。

處理的性質

提供 Sophos 根據協議並根據協議採購的服務。

數據傳輸和進一步處理的目的

供應商將視需要處理控制器個人資料、以根據合約執行服務、並依照 Sophos 的指示使用服務。

個人數據將被保留的期間，或者，如果不可能，用於確定該期間的標準

除附錄第 10 節另有規定外、供應商將在合約期間處理個人資料、除非另有書面協議。

對於傳輸到（子）處理器，還要指定處理的主題、性質和持續時間

供應商被授權使用供應商在執行協議或附錄時通知 Sophos 的子處理器。

C. 主管監督機構

如 3.4 增編附件 4 第節所述 。

附件二－ 技術和組織措施，包括確保數據安全的技術和組織措施

如增編附件 2 所述。

附件三 - 分處理器清單

不適用（各方已就管制委員會第 9(a)條同意選擇方案 2(一般授權)）。