SOPHOS
Cybersecurity made simple.

**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。如果本文件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：2022 年 1 月 20 日**

如果此數據處理附錄（ “**附錄**” ）明確地通過引用方式納入 Sophos Limited （在英國和威爾士註冊的公司，編號爲 2096520 ）之間的協議（ “**主要協議**” ）中，並且其註冊辦事處位於 The Pentagon、 Abingdon Science Park、 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。

## 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.aspx （ “**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爲客戶收集、處理和使用控制器數據。本增編規定了當事各方對此類數據處理的義務，並補充了主要協議的條款和條件。

1.4 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"** 係指 (i) 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"** ）； (ii) 電子隱私指令（歐盟指令 2002/58/EC ）；及 (iii) 任何及所有適用的國家數據保護法規，包括根據或依據 (i) 或 (ii) 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。

“**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 ）。

“**Controller Data**” （控制器數據）是指控制器根據適用的數據保護法律作爲控制器的所有個人數據。

“**最終客戶**” 在 OEM 協議中具有其含義。

“**歐洲**” ( 和 “歐洲” ) 指㈠歐洲經濟區 ( “**EEA**” ) 的成員國，和㈡在歐洲聯盟法律不再適用於聯合王國和聯合王國之日之後立即生效。

**“歐盟標準合同條款”或“歐盟 SCC ”** 是指根據歐洲議會條例 2016/679 和歐洲委員會執行決定 (EU) 2021/914 批准的歐洲委員會執行決定 2021/914 向第三國轉讓個人數據的標準合同條款；

**“歐盟控制器對處理器條款”**是指對歐盟 SCC 的第二單元條款；

**“ EU Processor to Processor Clauses”**（歐盟處理器對處理器條款）是指對歐盟 SCC 的模塊三條款。

“**託管 產品**”是 **指圖 3 中列出的產品**。

「**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、未經授權揭露或存取、 供應商根據本附錄處理的控制器數據。

“**UK Addendum**”（英國附錄）指附件中所列的歐盟 SCC 附錄（如果適用）。

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 供應商處理控制器數據的主題和期限，包括處理的性質和目的、要處理的控制器數據的類型以及數據主題的類別，應如下所述：(i) 本附錄； (ii) 主要協議； (iii) **附件 1 中的任何指示**； 及 (v) 根據第 4 條發出的客戶指示。

3.2 客戶有責任確保 (i) 控制器有合法的基礎處理供應商將代表其執行的控制器數據， (ii) 財務總監已取得客戶及供應商處理控制器數據所需之資料當事人之所有必要同意書（包括但不限於特殊類別數據）； 以及（ iii ）其在其他方面符合並將確保其指示供應商處理控制器資料時遵守適用的資料保護法律。

3.3 本增編的其餘規定說明了當事各方在財務主任數據方面的各自義務，其中包括：(i) 客戶是控制器，供應商是處理器（如果客戶是最終用戶）；或 (ii) 客戶是第三方控制器的處理器，如果客戶是 MSP 或 OEM ，供應商是子處理器。

## 4. 客戶指示

4.1 供應商應依照客戶的書面處理指示處理控制器資料、如條款中所述、 3.1 但以下情況除外：

(a) 如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、並暫停處理控制器資料。

## 5. 供應商的責任

5.1 處理控制器數據的所有供應商人員應接受有關其數據保護、安全和保密義務的充分培訓，並應遵守保密的書面義務。

5.2 供應商將自行承擔成本、實施適當的技術和組織措施、以確保符合風險的安全等級、並保護主計長資料免於個人資料外洩。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 供應商應遵循第 7 條中規定的要求，委聘任何子處理器來處理控制器數據。

5.4 供應商應遵循第 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必要的所有措施與行動、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所有發展。

5.6 供應商應提供客戶（或客戶是 MSP 或 OEM 、其控制器）所需的所有合理及時的協助、以進行資料保護影響評估、並在必要時、 請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 供應商應在本附錄終止或到期後的合理期間內刪除控制器的控制器數據（在適用的歐洲法律允許的情況下和在適用的範圍內）。

5.8 供應商應遵循第 6 條中規定的要求，向客戶（如果客戶是 MSP 或 OEM ，則爲其控制人）提供證明供應商遵守本附錄中規定的義務所必需的信息。

## 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。 供應商應在客戶要求下提供一份 SOC 2 稽核報告副本給客戶、此報告應受主要合約保密條款的規範、作為供應商的機密資訊。客戶確認並同意，編寫此類報告的第三方審計員（“**作者**”）不承擔對客戶或客戶審計員的任何責任或責任，除非客戶與作者另行簽訂了“維護責任”協議。供應商也應回應客戶提交給客戶的任何書面稽核問題、但客戶不得每年行使此項權利超過一次。

## 7. 子處理器

7.1 客戶同意供應商在本附錄日期的現有子處理器，這些子處理器列於 https://www.sophos.com/en-us/legal（下稱“**子處理器列表**”）。供應商不會在未事先通知客戶的情況下，將任何控制器數據的處理分包給任何其他第三方子處理器（每個子處理器都是“**新子處理器**”）。供應商會事先通知新增任何子處理器（包括其執行或將執行之處理程序的一般詳細資料）、您可以在子處理器清單中張貼此類新增的詳細資料、以發出通知。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：（ i ）供應商不會使用新的子處理器來處理控制器資料；或（ ii ）供應商無法或不願意這麼做。如發出第 (ii) 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。供應商將對新的子處理器實施數據保護條款，以保護控制器數據達到本附錄規定的相同標準，供應商對任何此類子處理器導致的違反本附錄的行爲負全部責任。

## 8. 第三方的詢問

8.1 供應商應向客戶（或者，如果客戶是 MSP 或 OEM ，則爲控制器）提供所有合理且及時的幫助，並由客戶承擔費用，以使客戶能夠對以下事項作出響應：(i) 任何資料的要求，而該等資料須根據適用的資料保護法行使其任何權利 ( 包括其存取權、更正權、反對權、刪除權及資料可攜性 ( 如適用 ) ) ； 及 (ii) 從資料當事人、規管人或其他第三方接獲有關處理財務總監資料的任何其他通訊、查詢或投訴。 如有任何此類要求、信件、查詢或投訴直接向供應商提出、供應商應立即通知客戶提供完整的詳細資料。

## 9. 國際數據傳輸

9.1 某些產品使客戶可以選擇是否將此類產品的控制器數據存放在以下數據中心中： (i) 歐洲經濟區 (ii) 英國或 (iii) 美國（ “**中央存儲位置**” ）。此選項在安裝、創建帳戶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 客戶確認並同意、無論所選的中央儲存位置為何（如適用）、控制器資料均可透過或匯出至其他司法管轄區（英國及歐洲經濟區內外）：(i) 針對惡意軟件、安全威脅和誤判分析以及研究和開發目的，向 Sophos 的全球技術人員和工程師團隊提供 (ii) ，以便提供技術和客戶支持、帳戶管理、計費和其他輔助功能，以及 (iii) 如第 3.1 條所述的文檔中所明確說明。

9.3 供應商不得轉移控制器數據（也不得允許控制器數據在或從其處處理） 歐洲以外的國家 / 地區、除非該國家 / 地區根據適用的資料保護法律被視為適當、否則供應商會採取必要措施、以確保傳輸符合適用的資料保護法律、包括但不限於、 使用歐盟 SCC （經不時修訂）。

9.4 如聯合王國不再受歐洲聯盟法律的約束，第 9.3 條所述的轉讓限制也適用於從歐洲經濟區向聯合王國轉讓財務主任數據。

9.5 如果第 9.3 條的適用是因爲供應商或供應商關係企業將在英國或歐洲經濟區以外的國家處理控制器數據，則在這種情況下（並且僅限於控制器數據的任何轉移， 根據適用的數據保護法律，允許進行此類轉讓的其他措施均不可用（例如，但不限於 對於控制器數據的任何轉移，如果在根據適用的數據保護法律被視爲對個人數據提供充分保護的國家 / 地區，或將其轉移給已根據適用的數據保護法律獲得具有約束力的公司規則授權的接收者）， 雙方同意：

(a) 對於從歐洲經濟區轉移的情況，歐盟控制器應適用處理器條款，並將此類歐盟 SCC 作爲參考併入本增編；

(b) 對於從英國轉移的情況，歐盟控制器對處理器條款應適用（並將此類歐盟 SCC 作爲參考併入本增編），條件是此類歐盟控制器對處理器條款應受英國增編的約束。

9.6 如果第 9.3 條的適用是因爲供應商或供應商關係企業將在英國或歐洲經濟區以外的國家處理控制器數據，則在此情況下（並且僅限於控制器數據的任何轉移， 根據適用的數據保護法律，允許進行此類轉讓的其他措施均不可用（例如，但不限於 根據適用的資料保護法律、轉移給被視為為個人資料提供適當保護的國家 / 地區的收件者、或轉移給已根據適用的資料保護法律獲得具約束力之企業規則授權的收件者）（如第 3.3(ii) 條所述）客戶爲第三方控制器的處理器，供應商爲子處理器，各方同意：

(a) 對於從歐洲經濟區轉出的歐盟處理器至處理器條款，應適用，並將此類歐盟 SCC 作爲參考併入本附錄中；

(b) 對於從英國轉出的歐盟處理器至處理器條款，應適用（並將此類歐盟 SCC 作爲參考併入本增編），條件是此類歐盟處理器至處理器條款應受英國增編的約束。

9.7 歐盟 SCC 的附錄應按以下附件 4 所列方式填寫。

9.8 對於每個模塊到歐盟 SCC （如果適用）：

(a) 第 7 條中的任擇對接條款不適用；

(b) 第 9 條下的備選案文 2 適用。 資料進口商應在子處理器清單的任何預期變更（透過新增或更換）前 30 天通知資料出口商。

(c) 在第 11 條中，任擇語文不適用；

(d) 就第 13(a) 條而言：

- 在歐盟成員國建立數據出口國時：負責確保數據出口者遵守條例 2016/679 關於數據轉移的監督機構將是建立數據出口者的主管監督機構，並應作爲主管監督機構。

(e) 就第 17 條而言，歐盟 SCC 應受建立數據出口國的歐盟成員國法律管轄；

(f) 爲了第 18(b) 條的目的，爭端將在建立數據出口國的歐盟成員國法院得到解決。

## 10. 持續時間

10.1 本增編由雙方簽署主要協議（或主要協議生效之日（如較晚生效）起生效，並持續至以下日期：(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。

11.2 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。 供應商對主要協議所規定的責任限制應在主要增編和本增編中綜合適用，因此對責任制度的單一限制應適用於主要協議和本增編。

11.3 本附錄應受英格蘭和威爾斯法律管轄並依其解釋、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 在與本數據處理附錄條款和各方訂立的任何 SCC 條款發生衝突的情況下，適用的歐盟 SCC 條款應優先。

SOPHOS
Cybersecurity made simple.

## 附件 1.
## 資料處理指示

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**
控制器數據將受以下基本處理活動的約束（請具體說明）：

1. 提供客戶根據主要協議並根據主要協議購買的產品
2. 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：**
控制器數據將在以下持續時間內處理（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**
主計長資料涉及下列類別的資料主題（請說明）：

數據主題包括由客戶或客戶的最終用戶通過產品向供應商提供（或根據其指示）數據的個人。

**(d) 個人資料的類型**
控制器數據涉及以下類別的數據（請具體說明）：

與通過產品、客戶或客戶最終用戶（如聯繫信息）提供給供應商的個人相關的數據

**(e) 特殊類別的數據 ( 如適用 )**
財務主任數據涉及以下特殊類別的數據（請具體說明）：

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
Cybersecurity made simple.

## 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。

A) 物理訪問控制。

- Sophos 具有物理訪問控制策略；
- 所有工作人員均攜帶身份證 / 出入證；
- 設施的入口受到出入證或鑰匙的保護；
- 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限制出入區，只有那些有明確業務需要的人員才能進入；
- 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受限制區域的出入；
- 個人的進入級別由高級工作人員批准，並每季度進行一次覈實；
- 接待處和 / 或保安人員在較大地點的入口處；
- 設施受到警報保護；
- 訪客會預先註冊、並保留訪客記錄。

B) 系統訪問控制。

- Sophos 具有邏輯訪問控制策略；
- 網絡在每個 Internet 連接上都受到防火牆的保護；
- 內部網絡根據應用敏感度由防火牆分割；
- 在所有防火牆上運行 ID 和其他威脅檢測和阻止控制；
- 過濾網絡流量是根據應用“最少訪問”原則的規則進行的；
- 只有在必要的範圍和期限內授權人員才能執行其工作職責，並每季度審查一次訪問權限；
- 對所有系統和應用程序的訪問由安全登錄過程控制；
- 個人有自己使用的唯一用戶 ID 和密碼；
- 密碼經過強度測試，並對弱密碼進行更改；
- 屏幕和會話在一段時間不活動後自動鎖定；
- Sophos 惡意軟件保護產品作爲標準安裝；
- 定期對 IP 地址和系統進行漏洞掃描；
- 系統會定期進行修補，並使用優先級系統來快速跟蹤緊急修補程序。

C) 數據訪問控制。

- Sophos 具有邏輯訪問控制策略；
- 只有在必要的範圍和期限內授權人員才能執行其工作職責，並每季度審查一次訪問權限；
- 對所有系統和應用程序的訪問由安全登錄過程控制；
- 個人有自己使用的唯一用戶 ID 和密碼；
- 密碼經過強度測試，並對弱密碼進行更改；
- 屏幕和會話在一段時間不活動後自動鎖定；
- 便攜式計算機使用 Sophos 加密產品進行加密；
- 寄件者在傳送任何外部電子郵件之前，必須考慮檔案加密。

D) 輸入控制。

- 對所有系統和應用程序的訪問由安全登錄過程控制；
- 個人有自己使用的唯一用戶 ID 和密碼；
- Sophos Central 產品使用傳輸層加密來保護傳輸中的數據；
- 客戶端軟件與後端 Sophos 系統之間的通信通過 HTTPS 執行，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。

E) 分包商控制。
- 擁有資料存取權的轉包商、在到職前及其後依規定進行 IT 安全性審查程序；
- 合同中包含根據分包商的職責而承擔的適當保密義務和數據保護義務。

F) 可用性控制。
- Sophos 保護其場所免受火災、水災和其他環境危害；
- 備用發電機可在停電時維持電源供應；
- 數據中心和服務器機房使用氣候控制和監控；
- Sophos Central 系統具有負載平衡功能，並在三個站點之間進行故障轉移，每個站點都運行兩個軟件實例，其中任何一個都可以提供完整服務。

G) 隔離控制。
- Sophos 維護並應用質量控制流程來部署新的客戶產品；
- 測試和生產環境是分開的；
- 新的軟件、系統和開發在發佈到生產環境之前進行了測試。

H) 組織控制。
- Sophos 擁有一個專用的 IT 安全小組；
- 風險與法規遵循團隊負責管理內部風險報告與控管、包括報告管理的關鍵風險；
- 事件響應流程及時識別並解決風險和漏洞；
- 每位新員工都負責數據保護和 IT 安全培訓；
- 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

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

**附件 4.**

**歐盟標準合同條款的參考數據**

**歐盟標準合同條款附錄 1**

**答：締約方名單**

**資料匯出器：**[*數據導出者的身份和聯繫詳細信息，包括負責數據保護的任何聯繫人*]

**客戶名稱**：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聯繫電子郵件：

聯繫人姓名 / 職位：根據主要協議提供給供應商

與根據本條款轉移的數據有關的活動：如上文第 3 條所述

角色（控制器 / 處理器）：控制器

**資料匯入程式：**[*數據進口商的身份和聯繫細節，以及其 / 其數據保護幹事和 / 或歐洲聯盟代表的身份和聯繫詳情*]

**姓名：**Sophos Limited（代表其歐盟及瑞士附屬公司）

**地址：**英國 OX14 3YP OX14 Abingdon 科學園五角大廈

註冊號碼：2096520

聯繫人姓名、職位和聯繫方式： dataprotection@sophos.com

與根據本條款轉移的數據有關的活動：如上文第 3 條所述。

角色（控制器 / 處理器）： 處理器

**B. 轉讓說明**

*傳輸個人資料的資料對象類別：*

如上文 C 節附件 1 所述

*傳輸的個人資料類別：*

如上文 D 節附件 1 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：*

如上文 E 節附件 1 所述。

*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*

如上文 A 節附件 1 所述。

*數據傳輸和進一步處理的目的*

如上文 A 節附件 1 所述。

*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*

在訂約期間內。

*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*

如上文第 3 條所述。

**主管監督機構**

見上文第 9.8 條

**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**[1]

這些措施載於 上文附件 2。

**附件三 - 分處理器清單**[2]

由於第 9(a) 條並 _無選擇第 1 項，因此毋須填寫。

[1]除第四單元外，所有單元都必須完成附件二。
[2]附件 III 僅適用於選擇第 9(a) 條第 1 款的第二單元（將控制器轉移到處理器）和第三單元（將處理器轉移到處理器）。