Microsoft 採購部

供應商安全與隱私保證 (SSPA) 計劃指南

版本 8

2022 年 6 月

簡介

在 Microsoft，我們認為隱私權是一項基本權利。幫助在這個地球上的每一個人到每一個組織，都能貢獻更多、成就更大是我們堅定不移的使命，因此，我們每天都在努力贏得並維持客戶對我們的信任。強大的隱私保護和安全實踐對於踐行我們的使命至關重要，對於不辜負客戶的信任更是極其重要，因此，我們在眾多司法轄區均依法採取隱私保護措施。Microsoft 隱私與安全政策中所涵蓋的標準反映了我們作為一家公司的價值觀，這些標準也同樣適用於代表我們處理 Microsoft 資料的供應商（如貴公司）。

供應商安全與隱私保證（「**SSPA**」）計劃是 Microsoft 推出的企業計劃，旨在以 Microsoft 供應商資料保護要求（「**DPR**」）（請參見 Microsoft.com/Procurement 中的 SSPA 介紹）的形式，向供應商傳達 Microsoft 基本的資料處理說明。請注意，除 SSPA 以外，供應商還須遵守與供應商接洽的 Microsoft 集團在企業層面決定和傳達的其他要求。

DPR 中提供了關於 SSPA 關鍵術語的定義。如需瞭解關於本計劃的更多資訊，請參閱我們的常見問題 (FAQ)，也可致函聯絡我們的全球團隊：SSPAHelp@microsoft.com。

SSPA 計劃概覽

SSPA 是由 Microsoft 採購部、企業對外和法律事務部及企業安全部合作推出的一項計劃，旨在確保我們的供應商遵守隱私和安全原則。

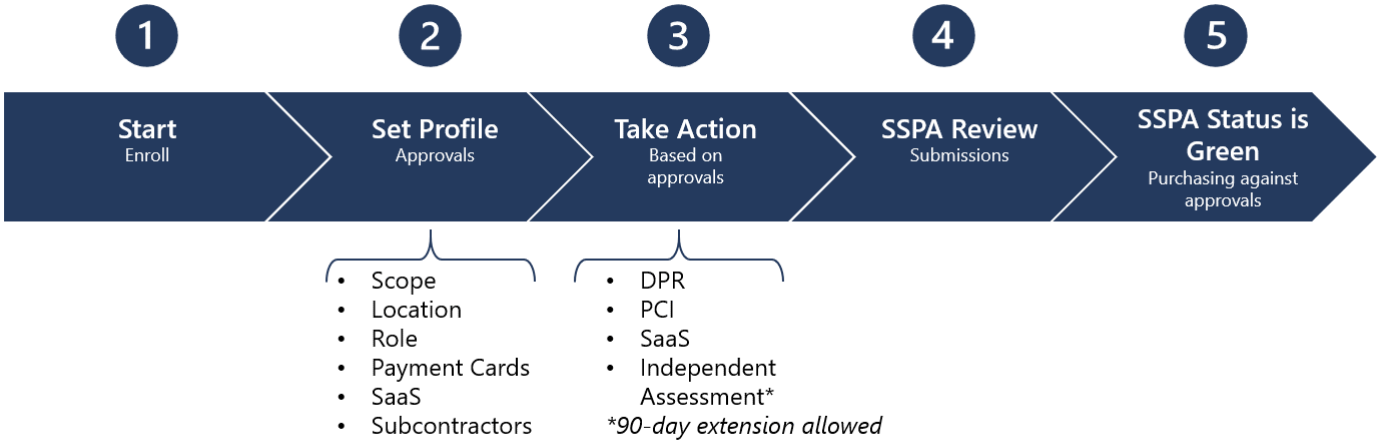
根據與 Microsoft 簽訂之合約條款（如採購訂單條款、主協議），SSPA 的範圍涵蓋為履行業務（包括提供服務、軟體授權、雲端服務，以下簡稱為「**執行**」、「**履行**」或「**業務履行**」）而處理個人資料和/或 Microsoft 機密資料的全球所有供應商。

SSPA 使供應商能夠根據產品和/或服務合約，在資料處理檔案中選擇要履行的相應業務。供應商所做選擇會觸發相應要求，然後根據要求向 Microsoft 提供合規保證。

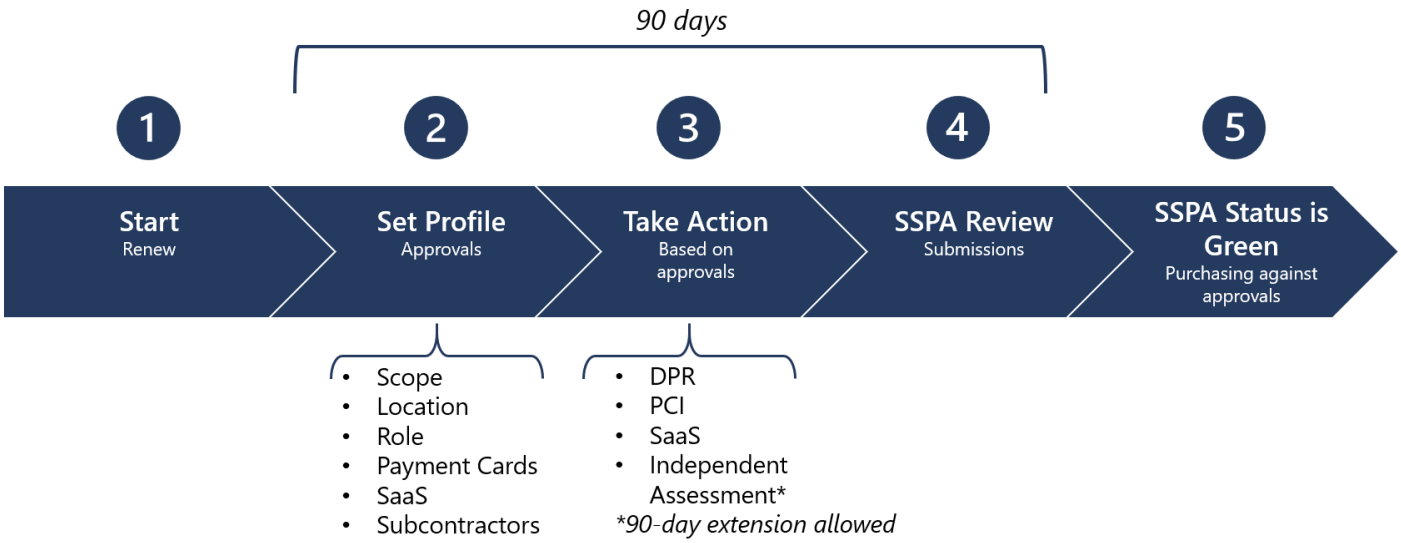
所有註冊的供應商每年應完成遵守 DPR 的自我證明。資料處理檔案中將確定是否發佈了完整的 DPR，或細分要求是否適用。若供應商負責處理 Microsoft 認為具有高風險的資料，還需遵守其他要求，如提供單獨的合規驗證。Microsoft 發佈的子處理商清單中的供應商，還需提供單獨的合規認證。

重要資訊：合規活動決定了 SSPA 的狀態為綠色（合規）或紅色（不合規）。Microsoft 採購工具可驗證 SSPA 的狀態是否為綠色（針對 SSPA 範圍內的每個供應商），然後才允許供應商承攬業務。

SSPA 流程圖 – 新供應商註冊



SSPA 流程圖 – 供應商年度續期



SSPA 的範圍

為幫助判斷您（供應商）處理的是否為個人資料和/或 Microsoft 機密資料，請參見下表中的示例清單。請注意，這些僅為示例，而非詳盡清單。

注：鑑於所處理之資料的機密性，除此清單外，Microsoft 業務擁有者可以要求在此清單之外進行其他註冊。 。

按資料類別劃分的個人資料

示例包括但不限於：

敏感資料
與兒童有關的資料
遺傳資料、生物特徵資料或健康資料
種族或族裔
政治、宗教或哲學信仰、觀點和立場
工會會員資格
自然人的性生活或性取向
移民身份（簽證、工作授權等）
政府頒發的身份證件（護照；駕照；簽證；社會安全號碼；國民身份證號）
精確的使用者定位資料（300 米以內）
個人銀行帳號
信用卡號和到期日
客戶內容資料
文件、照片、影片、音樂等
輸入的關於產品或服務的評論和/或評級
問卷調查回答
瀏覽歷史記錄、興趣和我的最愛
字跡、打字和語音（語音/音訊和/或聊天/機器人）
憑證資料（密碼、密碼提示、使用者名稱、用於識別個人身份的生物特徵資料）
與支援案例相關的客戶資料

獲取和生成的資料
非精確的位置資料
IP 位址
設備首選項和個人化資訊
網站服務使用情況、網站點按率跟蹤
社交媒體資料、社交關係圖譜
來自連線設備（如健身監測器）的活動資料
聯絡人資料，如姓名、地址、電話號碼、電郵地址、出生日期、家屬和緊急聯絡人
欺詐和風險評估、背景調查
保險、養老金、福利詳情
求職者簡歷、面試筆記/回饋
Metadata and telemetry
帳戶資料
付款方式資料
信用卡號和到期日
銀行路由資訊
銀行帳號
信用申請或信貸額度
稅務文件和稅號
投入或支出資料
企業卡
最終使用者假名資訊 (EUPI) （由 Microsoft 建立的識別碼，用於識別 Microsoft 產品和服務的使用者）
全域唯一識別碼 (GUID)
Passport 使用者 ID 或唯一識別碼 (PUID)
散列最終使用者識別資訊 (EUII)
會話 ID
設備 ID
診斷資料
登入資料

Online Customer Data
Microsoft online enterprise customer (example: Azure tenant, M365 tenant…)
Microsoft consumer customer (example: Xbox Live, OneDrive Consumer, …)
Microsoft enterprise customer (on premises customer)
Support data (example: Customer originates a ticket)
Account data (example: billing data, e-commerce)
Survey/Event Registration/Training

按資料類別劃分的 Microsoft 機密資料

示例包括但不限於：

高度機密資料
關於 Microsoft 產品或 Microsoft 產品組件開發、測試或製造的資訊 *在任何管道進行商業銷售的被視為「**Microsoft 產品**」的 Microsoft 軟體、線上服務或硬體*
Microsoft 設備會預先發佈行銷資訊
受 SEC 規定約束的未公佈 Microsoft 企業財務資料
機密資料
代表 Microsoft 透過任何方式分發的 Microsoft 產品授權密鑰
關於 Microsoft 內部業務線 (LOB) 應用程式開發或測試的資訊
Microsoft 預發佈的關於 Microsoft 軟體和服務（如 Office、SQL、Azure 等）的行銷材料
關於任何 Microsoft 服務或產品（如設備）的書面、設計、電子版或列印的文件（流程或規程指南、配置資料等）

重要資訊：對於未包含在此清單中的資料，Microsoft 企業所有者可能需要予以分享。

資料處理檔案

Microsoft 供應商對其 SSPA 資料處理檔案具有控制權。

這使供應商可決定希望有資格履行哪些業務。請仔細注意所做選擇，為獲得審批，請斟酌必須完成的合規活動。**請參見下文「保證要求」部分和附錄 A。**

Microsoft 業務組僅可在資料處理活動與供應商獲得的審批相匹配的情況下，與供應商建立合作關係。

在無開放任務的情況下，供應商可在一年中隨時更新其資料處理檔案。在進行更改時，將發佈相應的活動任務，而在獲得審批之前，必須完成這些任務。當前已完成的審批將一直適用，直至完成新發佈的要求。

若在規定的 90 日期限內未完成新執行的任務，SSPA 狀態將變為紅色（不合規），而供應商帳戶則面臨被 Microsoft 應付帳款系統停用的風險。

資料處理審批	
1	資料處理範圍 ▪ 機密資料 ▪ 個人資料、機密資料
2	資料處理地點 ▪ 於 Microsoft 或客戶處 ▪ 在於供應商處
3	資料處理角色 ▪ 控制**者**（獨立或聯合控制**者**） ▪ 處理**商** ▪ 子處理**商**（由 Microsoft 指定）
4	支付卡處理 ▪ 是 ▪ 不適用
5	軟體即服務 ▪ 是 ▪ 不適用
6	使用分包商 ▪ 是 ▪ 不適用

審批考量因素

資料處理範圍

機密資料

若供應商履行的業務中僅涉及處理 Microsoft 機密資料，請選擇此審批選項。

若您選擇此審批選項，您將沒有資格承接個人資料處理業務。

個人資料、機密資料

若供應商履行的業務中涉及處理個人資料和 Microsoft 機密資料，請選擇此審批選項。

處理地點

於 Microsoft 或客戶處
若供應商履行的業務涉及在 Microsoft 的網路環境（其中員工使用 *@microsoft.com* 存取憑據）或 Microsoft 客戶的網路環境中處理資料，請選擇此審批選項。

在以下情況下，請勿選擇此選項：

- 供應商負責管理 Microsoft 指定的離岸設施 (OF)。
- 供應商應向 Microsoft 提供資源，且他們時而在 Microsoft 網路內和網路外進行辦公。網路外處理地點被認為於「供應商處」。

在供應商處
若「 於 Microsoft 處或客戶處」（如上所述）的條件不適用，請選擇此選項。

資料處理角色

控制者（包括獨立和聯合控制**者**）

若供應商履行業務的<u>所有</u>方面均符合關於控制方資料處理角色的定義（請參見 DPR），請選擇此審批選項。

若您選擇此審批選項，將沒有資格使用指定的「處理**商**」角色處理個人資料。若供應商同時是 Microsoft 的處理**商**和控制**者**，則請勿選擇「控制**者**」，而要選擇「處理**商**」。

處理商

此為代表 Microsoft 處理資料的最常見資料處理角色。請參閱 DPR，查看關於處理**商**的定義。

子處理商

子處理**商**是在 Microsoft 作為處理**商**的情況下，由 Microsoft 聘用履行業務的第三方，履行的業務包括處理 Microsoft 個人資料。供應商不得自我認定為 Microsoft 的子處理**商**，因為需要由內部隱私團隊進行預先審批。在 Microsoft 作為處理**商**的情況下，供應商才可作為子處理**商**，且供應商僅可處理符合條件的企業個人資料類型。子處理**商**需要遵守額外合約和合規要求，包括資料保護補充合同和單獨評估要求（見下文）。

支付卡處理

若由供應商代表 Microsoft 處理的資料中包含任何用於支援信用卡或其他支付卡處理的資料，請選擇此審批選項。

透過獲得此項審批，供應商可承接支付卡處理業務。

軟體

對於所有購買軟體的情況，Microsoft 採購部會透過客戶吸納流程指導買方，其中包括各種檢查，比如查看 SSPA 鑒別分類，以確定提供軟體的供應商是否屬於 SSPA 管理的範疇。（Microsoft 產品買方可

參閱內部 ProcureWeb 軟體和雲端服務頁面中概述的步驟，瞭解更多詳情）。若 SSPA 要求，供應商還需確定檔案中的「軟體即服務」(SaaS) 選擇適用。對於註冊加入 SSPA 的供應商，在 Microsoft 供應商合規入口網站中完成資料處理檔案後，完成此項要求。

出於遵守 SSPA 之目的，可寬泛地看待軟體即服務，其中還可包括平台即服務 (PaaS) 和基礎設施即服務 (IaaS)。（如需瞭解關於軟體即服務的更多資訊，請參見此說明。）

軟體即服務 (SaaS)

使用者可利用軟體即服務 (SaaS) 透過網際網路連線到基於雲端的應用，然後即可使用這些應用。

Microsoft 將**軟體即服務 (Software as a Service, SaaS)** 定義為：基於一對多模型中使用的通用程式碼的軟體，按需付費或基於使用名額進行訂閱。雲端服務提供者負責開發和維護基於雲端的軟體、提供自動軟體更新，以及按照一對多、按需付費模式透過網際網路向客戶提供軟體。透過採用這種軟體交付和授權方式，使用者可透過訂閱線上存取軟體，而無需購買並安裝到每台電腦上。

注：若個人資料或 Microsoft 機密資料由第三方平台託管，則多數軟體即服務供應商均需要在 Microsoft 供應商合規入口網站上新增分包商審批。

使用分包商

若供應商使用分包商履行此業務（請參見 DPR，瞭解具體定義），請選擇此審批選項。

其中也包括自由職業者（請參見 DPR）。

保證要求

基於檔案審批的要求

在資料處理檔案中選擇的審批選項有助於 SSPA 評估您在執行 Microsoft 業務時的風險等級。SSPA 合規要求因資料處理檔案的內容和相關審批選項而異。本節主要解釋不同的 SSPA 要求。

此外，還有一些審批組合可能會提高或降低合規要求。這些組合如附錄 A 中所示，在完成檔案後，即可等待審批，然後執行 Microsoft 供應商合規入口網站的內容。透過請求 SSPA 團隊審查，通常可驗證您的方案是否適合此框架。

採取的行動：在附錄 A 中查找關於審批檔案的說明，並查看相應的保證要求和單獨保證選項（如適用）。

重要資訊：若您的檔案中包括軟體即服務 (SaaS)，則要求額外提供分包商、網站託管或支付卡保證。

遵守 DPR 的自我證明

所有註冊加入 SSPA 的供應商均須在收到要求後的 90 日內完成遵守 DPR 的自我證明。此項要求通常每年下發一次，但若資料處理檔案在年中時更新，則會增加頻次。若超出 90 日的期限，供應商帳戶中的 SSPA 狀態將變為紅色（不合規）。在 SSPA 狀態變為綠色（合規）之前，將無法處理業務範圍內新的採購訂單。

新註冊的供應商必須完成發佈的要求，以確保在開始履行業務之前，SSPA 的狀態為綠色（合規）。

重要資訊：SSPA 團隊無權針對此任務提供延期。

授權代表需完成自我證明，並確保已從主題領域專家處獲得了足夠的資訊，能夠自信應對每項要求。此外，透過在 SSPA 表單中新增聯絡人姓名，即證明他們已閱讀並理解了 DPR。供應商可在線上工具中新增其他聯絡人，協助完成各項要求。

授權代表（請參見 DPR，瞭解具體定義）負責：

1. 確定適用的要求。
2. 回應每項適用的要求。
3. 在 Microsoft 供應商合規入口網站上簽署並提交證明。

適用性

供應商應回應根據資料處理檔案發佈的所有適用的 DPR 要求。預計在發佈的要求中，有少數會不適用於供應商向 Microsoft 提供的產品或服務。供應商可將此類要求標記為「不適用」並附上詳細備註，以供 SSPA 審查人員驗證。

SSPA 團隊會參照發佈的要求，審查針對 DPR 提交的內容，以確定有無選擇為「不適用」、「與當地法律衝突」或「與合約衝突」的任何要求。SSPA 團隊可能會要求供應商詳細說明其中一項或多項選擇。僅在提供輔助參考資料且明確存在衝突的情況下，才會認可相關要求確實與當地法律和合約存在衝突。

獨立評估要求

請參見附錄 A 中的「審批要求」，瞭解觸發此項要求的資料處理審批。

供應商可選擇透過更新資料處理檔案更改審批選項。但若供應商的資料處理角色為「子處理商」，則供應商無法更改此審批選項，並需要每年執行一次獨立評估。

在需要執行獨立合規驗證的情況下，為獲得審批，供應商需要選擇獨立評估方驗證其是否遵循 DPR。評估方需要編制一份建議函，以便向 Microsoft 提供合規保證。此函必須毫無保留地闡明所有不合規問題，且必須將所有問題妥善解決並整治後，才可將確認函提交到 Microsoft 供應商合規入口網站，供 SSPA 團隊審查。評估方可下載經核准的建議函範本（隨附於「首選評估方」PDF 文件中，請點按此處查看）。

若供應商選擇不使用獨立評估方驗證是否遵守 DPR（在適用情況下，如軟體即服務供應商、網站託管服務供應商、採用分包商的供應商），**附錄 A** 中提供了認可的認證替代方案。ISO 27701（隱私認證）和 ISO 27001（安全認證）與 DPR 密切相關，可予以採用。

若供應商是美國的醫療服務供應商或受保實體，我們將接受關於隱私和安全範圍的 HITRUST 報告。

若情況超出標準規定的範疇，需要啟動額外的盡職調查，則 SSPA 會每年執行一次獨立評估。例如在隱私或安全部門要求的情況；需要對資料洩露事故的補救措施進行驗證的情況；或要求自動行使資料主體權利的情況。

關於如何執行此項要求的指南：

1. 必須由經過充分技術訓練且掌握關於合規評估專業知識的評估人員執行此項評估任務。
2. 評估方必須隸屬於國際會計師聯合會 (IFAC) 或美國註冊會計師協會 (AICPA)，或必須持有其他相關隱私和安全機構頒發的認證，例如國際隱私專家協會 (IAPP) 或資訊系統審計與控制協會 (ISACA)。
3. 評估方必須參照最新版 DPR，其中包括支援每項要求所需的證據。**供應商需要向評估方提供最近經核准的對 DPR 證明的回覆。**
4. 對於新註冊的供應商，評估方需要檢驗資料處理控制流程的設計。在所有其他情況下，評估方將檢驗控制流程的有效性。
5. 評估任務的範圍僅限於與供應商業務履行有關的個人資料和/或 Microsoft 機密資料。
6. 評估任務的範圍僅限於根據供應商帳號中收到的請求執行的所有業務範圍內的資料處理活動。若供應商一次選擇多個供應商帳號，**證明函中必須包括評估中包含的供應商帳號清單和相關地址。**
7. 向 SSPA 提交的函件中不得包括供應商無法滿足書面資料保護要求的任何聲明。在信函提交前，必須妥善糾正問題。

SSPA 提供了一份首選評估方清單，供您查閱。這些公司對於執行 SSPA 評估非常熟悉。供應商需要承擔評估費用；具體費用將因資料處理的規模和範圍而異。

PCI DSS 認證要求

支付卡行業資料安全標準 (Payment Card Industry Data Security Standard, PCI DSS) 是開發健全的支付卡資料安全標準的框架，其中包括安全事故的預防、發現及適當應對措施。此框架由 PCI 安全標準委員會（一個自律組織）開發。PCI DSS 要求旨在識別技術和流程漏洞，以防對處理的持卡人資料安全造成風險。

Microsoft 必須遵守這些標準。若供應商代表 Microsoft 處理支付卡資訊，我們會要求供應商提交遵守這些標準的證明。請諮詢 PCI 安全標準委員會，瞭解由 PCI 組織制定的要求。

根據處理的交易量，供應商需要提交由合格的安全評估方出具的合規認證，或可填寫自我評估調查問卷表。

支付卡品牌針對評估類型設定了最低標準，通常為：

- 1 級：提供第三方評估機構 PCI AOC 認證
- 2 級或 3 級：提供由供應商官員簽署的 PCI DSS 自我評估調查問卷 (SAQ)。

提交適用且符合 PCI 要求的認證。

軟體即服務要求

對於符合資料處理檔案中關於軟體即服務定義的供應商，需要提供有效的 ISO 27001 認證（若 Microsoft 雲端服務協議中要求）。

SSPA 審查人員將驗證您提交的內容是否符合合約義務。

請勿提交資料中心認證。我們希望所提交的 ISO 27001 認證適用於您與 Microsoft 簽訂之合約中所述的軟體服務。

使用分包商

Microsoft 認為，使用分包商是一個高風險因素。若供應商使用分包商處理個人資料和/或 Microsoft 機密資料，則必須如實披露所使用的分包商。此外，供應商還應披露每個分包商在哪個國家處理個人資料。

資料洩露事故

若供應商意識到發生隱私或安全資料洩露事故，供應商必須按照 DPR 中的詳細說明通知 Microsoft。請參見附錄 B 中的適用定義。

請造訪 SupplierWeb 或傳送電郵至 SuppIR@microsoft.com，報告資料洩露事故

務必包括：

- 發生資料洩露事故的日期：
- 供應商名稱：
- 供應商編號：
- 需要通知的 Microsoft 聯絡人：
- 相關採購訂單（如適用/可用）：
- 資料洩露事故摘要：

附錄 A

基於檔案審批的要求

#	檔案	保證要求	單獨的保證選項
1	**範圍**：個人資料、機密資料 **資料處理地點**：於 Microsoft 或客戶處 **在資料處理過程中的角色**：**處理商**或**控制者** **資料類別**：機密資料**或**高度機密資料 **支付卡**：不適用 **軟體即服務**：不適用 **使用分包商**：不適用 **網站託管**：不適用	遵守 DPR 的自我證明	
2	**範圍**：機密資料 **資料處理地點**：**於**供應商處 **在資料處理過程中的角色**：不適用 **資料類別**：機密資料 **支付卡**：不適用 **軟體即服務**：不適用 **使用分包商**：不適用 **網站託管**：不適用	遵守 DPR 的自我證明	
3	**範圍**：機密資料 **資料處理地點**：**於**供應商處 **在資料處理過程中的角色**：處理商 **資料類別**：高度機密資料 **支付卡**：不適用 **軟體即服務**：不適用 **使用分包商**：不適用 **網站託管**：不適用	遵守 DPR 的自我證明 **以及** 單獨合規保證	單獨的保證選項： 1. 遵守 DPR 的自我證明，**或** 2. 提交 ISO 27001

#	檔案	保證要求	單獨的保證選項
4	**範圍：**個人資料、機密資料 **資料處理地點：於**供應商處 **在資料處理過程中的角色：**處理商 **資料類別：**高度機密資料 **支付卡：**不適用 **軟體即服務：**不適用 **使用分包商：**不適用 **網站託管：**不適用	遵守 DPR 的自我證明 **以及** 單獨合規保證	單獨的保證選項： 1. 完成關於 DPR 的單獨評估， 2. 關於 DPR 第 A-I 節和 ISO 27001 的單獨評估， **或** 3. 提交 ISO 27701 **和** ISO 27001 認證
5	**範圍：**個人資料、機密資料 **資料處理地點：於**供應商處 **在資料處理過程中的角色：**處理商 **資料類別：**機密資料 **支付卡：**不適用 **軟體即服務：**不適用 **使用分包商：**不適用 **網站託管：**不適用	遵守 DPR 的自我證明	
6	**範圍：**個人資料、機密資料 **資料處理地點：於**供應商處 **在資料處理過程中的角色：控制者** **資料類別：**高度機密資料或機密資料 **支付卡：**不適用 **軟體即服務：**不適用 **使用分包商：**不適用 **網站託管：**不適用	遵守 DPR 的自我證明	

#	檔案	保證要求	單獨的保證選項
7	**範圍：**個人資料、機密資料 **資料處理地點：**任何 **在資料處理過程中的角色：**子處理**商**（此角色由 Microsoft 確定 – 檔案中將顯示「子處理**商**是否獲得審批：是」） **資料類別：**高度機密資料或機密資料 **支付卡：**不適用 **軟體即服務：**不適用 **使用分包商：**不適用 **網站託管：**不適用	遵守 DPR 的自我證明 **以及** 單獨合規保證	單獨的保證選項： 1. 完成關於 DPR 的單獨評估， 2. 關於 DPR 第 A-I 節和 ISO 27001 的單獨評估， **或** 3. 提交 ISO 27701 和 ISO 27001

#	檔案	保證要求	單獨的保證選項
新增軟體即服務、分包商、網站託管所產生的影響			
8	**範圍：**個人資料、機密資料 **資料處理地點：於**供應商處 **在資料處理過程中的角色：**處理**商** **資料類別：**高度機密資料或機密資料 **支付卡：**不適用 **分包商：**「是」或 **軟體即服務：**「是」或 **網站託管：**「是」	遵守 DPR 的自我證明 **以及** 單獨合規保證	單獨的保證選項： 1. 完成關於 DPR 的單獨評估， 2. 關於 DPR 第 A-I 節和 ISO 27001 的單獨評估， **或** 3. 提交 ISO 27701 和 ISO 27001
9	**範圍：**個人資料、機密資料 **資料處理地點：** 於供應商處 **在資料處理過程中的角色：控制者** **資料類別：**高度機密資料或機密資料 **支付卡：**不適用 **分包商：**「是」或 **軟體即服務：**「是」或 **網站託管：**「是」	遵守 DPR 的自我證明	

#	檔案	保證要求	單獨的保證選項
其他支付卡和軟體即服務保證要求			
10	上述任何檔案和**支付卡**要求	上述任何適用要求**和**支付卡行業保證要求	提交 PCI DSS 認證
11	上述任何檔案和**軟體即服務 (SaaS)** 要求	適用的上述要求**和**提交合約中要求的 ISO 27001 認證 (涵蓋功能服務)。	提交包含所提供服務功能涵蓋範圍的 ISO 27001 認證。