Microsoft 供應商數據保護要求

適用性

Microsoft 供應商數據保護要求（「**DPR**」）適用於所有 Microsoft 供應商，根據供應商與 Microsoft 達成的合同條款（如，採購訂單條款、主協議）規定，處理與供應商執行業務（例如，提供服務、軟件許可、雲端服務）相關的 Microsoft 個人數據或 Microsoft 機密數據。（以下統稱「**執行**」）。

- 若 DPR 包含的要求與供應商與 Microsoft 達成的合同協議中規定的要求出現衝突，則以 DPR 為準，除非供應商在合同中確定了取代適用數據保護要求的正確條款（在這種情況下，合同條款優先）。
- **若**此處包含的要求與任何法律或法定要求出現衝突，則以法律或法定要求為優先。
- **若** Microsoft 供應商作為控制者運作，則 DPR 中的要求對該供應商可有所放寬。
- **若** Microsoft 供應商不處理 Microsoft 個人數據而僅處理 Microsoft 機密數據，則對於此 DPR 而言，對該供應商要求可有所放寬。

國際數據傳輸

在不限制供應商其他義務的情況下，除非 Microsoft 提供事先書面批准，否則供應商不得對 Microsoft 個人數據進行任何國際傳輸，並且在任何情況下，供應商都應遵守數據保護要求，包括標準合同條款，或者由 Microsoft 自行決定，採用由適當的數據保護機構或歐盟委員會批准的其他適當的跨境傳輸機制（如適用），並由 Microsoft 採用或同意。(i) 歐盟委員會採用或歐洲數據保護監督機構採用並經歐盟委員會批准的後繼標準合同條款，(ii) 英國根據英國《通用聯邦數據保護法》，(iii) 瑞士根據《瑞士聯邦數據保護法》，或 (iv) 由瑞士、英國和歐盟/歐洲經濟區組成的司法管轄區以外的司法管轄區的政府正式採用的管理個人數據國際傳輸的條款，應納入和自採用之日起對供應商具有約束力。供應商還應確保任何及所有子處理方（定義見標準合同條款）也符合要求。

關鍵定義

本 DPR 中使用的以下術語具有以下含義。 在整個 DPR 中使用的「包括」、「例如」、「如」、「例子如」等後方所接的範例應解釋為包含「但不限於」，除非透過「只」或「僅」等詞語限定。有關更多定義，請參閱本文件末尾的詞彙表。

「**控制者**」是指確定處理個人數據的目的和方式的實體。 「控制者」包括企業、控制者（該術語在 GDPR 中定義）以及數據保護法中的等效術語，視上下文要求而定。

「**Cookies**」是網站和／或應用程序存儲在設備上的小型文本文件，其中包含用於識別數據主體或設備的資料。

「**數據事件**」是指 (1) 違反安全規定，導致供應商或其分包商傳輸、存儲或以其他方式處理的 Microsoft 個人數據或 Microsoft 機密數據的意外或非法破壞、丟失、更改、未經授權的披露或訪問，或 (2) 與供應商處理 Microsoft 個人數據或 Microsoft 機密數據相關的安全漏洞。

「**數據主體**」是指可以直接或間接識別的可識別自然人，特別是透過引用諸如姓名、識別號、位置數據、網上標識符或特定於物理的一個或多個因素等標識符 該自然人的生理、遺傳、心理、經濟、文化或社會身份。

「**數據主體權利**」是指數據主體在法律要求的情況下訪問、刪除、編輯、導出、限製或反對處理該數據主體的 Microsoft 個人數據的權利。

「**法律**」是指具有管轄權的任何政府機構（聯邦、州、地方或國際）的所有適用法律、規則、詔令、法令、決定、命令、法規判決、守則、法令、決議和要求。 「**非法**」是指任何違反法律的行為。

「**Microsoft 機密數據**」是指任何信息，如果透過機密性或完整性方式受到損害，可能會給 Microsoft 造成重大的聲譽或財務損失。 這包括 Microsoft 硬件和軟件產品、內部業務線應用程序、預發佈營銷材料、產品許可證密鑰以及與 Microsoft 產品和服務相關的技術文檔。

「**Microsoft 個人數據**」是指由 Microsoft 或代表 Microsoft 處理的任何個人數據。

「**個人數據**」是指與數據主體相關的任何信息以及構成法律規定的「個人數據」或「個人信息」的任何其他信息。

「**過程**」是指對任何 Microsoft 個人數據或機密數據執行的任何操作或一組操作，無論是否透過自動方式，例如收集、記錄、組織、結構化、存儲、改編或更改、檢索、諮詢、使用 、透過傳輸、傳播或以其他方式提供的披露、對齊或組合、限制、刪除或破壞。 「正在處理」和「已處理」將具有相應的含義。

「**處理商**」是指代表另一個實體處理個人數據的實體，包括服務提供商、處理者（該術語在 GDPR 中定義）以及數據保護法中的等效術語，視上下文而定。

「**分包商**」是指供應商將其與涵蓋其績效的合同相關的義務委託給其的第三方，包括未直接與 Microsoft 簽訂合同的供應商附屬公司。

「**子處理商**」是指 Microsoft 聘請執行的第三方，其中執行包括對 Microsoft 作為處理方的 Microsoft 個人數據的處理。

供應商回應

供應商每年使用 Microsoft 管理的網上服務確認遵守這些要求。 請參閱 SSPA 計劃指南以了解如何管理合規性。

#	Microsoft 供應商數據保護要求	合規證明
	A 節： 管理	
1	Microsoft 與供應商之間的每份適用協議（例如，主協議、工作說明、採購訂單和其他訂單）都包含有關 Microsoft 機密和個人數據的隱私和安全數據保護語言（如適用），包括禁止出售 Microsoft 與供應商之間的直接業務關係之外的個人數據和 Microsoft 個人數據的處理。 對於作為與性能相關的處理商或分處理商營運的公司，關於 Microsoft 個人數據，協議必須包括處理的主題和持續時間、處理的性質和目的、Microsoft 個人數據的類型和類別數據主體和 Microsoft 的義務和權利。	供應商必須出示 Microsoft 與供應商之間的適用合同。 對於處理商和子處理商，處理說明包含在適用的協議中（例如，工作說明書、採購訂單）。 備註： 有進行中採購訂單的公司可能會在採購流程的後期添加對處理活動的必要描述。
2	如果 Microsoft 確認您的約定履行子處理商角色，供應商必須與 Microsoft 簽訂適用的數據保護協議。 備註： Microsoft 將在適用時將此指定發佈到您的個人資料中。	標準合同條款、網上客戶數據附錄和／或供應商和合作夥伴專業服務數據處理附錄。
3	將遵守 DPR 的責任和義務分配給公司內的指定人員或團體。	指定負責確保遵守 Microsoft 供應商 DPR 的個人或團隊的角色。 描述此人或組的權限和責任的文件，證明其具有隱私和／或安全角色。
4	為可以訪問供應商處理的與績效或 Microsoft 機密數據相關的個人數據的員工建立、維護和執行年度隱隱私和安全培訓。 如果您的公司沒有準備好的內容，您可以使用此腳本大綱並針對您的公司進行調整。 備註： 供應商人員可能需要完成 Microsoft 部門提供的額外培訓。	可提供年度考勤記錄，並可根據要求提供予 Microsoft。 培訓內容包括隱隱私和安全原則。 遵守培訓要求的文件將包括與隱隱私監管要求、安全義務以及遵守適用合同要求和義務相關的培訓證據。

#	Microsoft 供應商數據保護要求	合規證明
	A 節： 管理（續）	
5	僅根據 Microsoft 的書面說明處理 Microsoft 個人數據，包括將 Microsoft 個人數據傳輸到第三國或國際組織的情況，除非法律要求這樣做； 在這種情況下，處理商或子處理商（供應商）應在處理之前通知控制者（微軟）該法律要求，除非該法律基於公共利益的重要理由禁止此類資料。	供應商以電子方式編譯和維護所有 Microsoft 記錄的說明（例如，協議、工作說明或訂單文檔），並將其保存在供應商員工和參與績效的承包商易於獲取的位置。
	B 節： 須知	
6	供應商在代表 Microsoft 收集個人數據時必須使用 Microsoft 隱私聲明。 隱私聲明必須顯而易見並且可供數據主體使用，以幫助他們決定是否將其個人數據提交給供應商。 備註： 如果您的公司是處理活動的控制者，您將發佈自己的隱私聲明。	供應商使用指向目前已發佈的 Microsoft 隱私聲明的 fwdlink。 隱私聲明發佈在將收集用戶個人數據的任何環境中。 如果適用，可以使用離線版本，並在數據收集之前提供。 使用的任何離線隱私聲明都是最新的、已發佈的版本，並且日期正確。 對於 Microsoft 員工服務，使用 Microsoft 數據隱私聲明。
7	透過即時或錄製的語音通話收集 Microsoft 個人數據時，供應商必須準備好與數據主體討論適用的數據收集、處理、使用和保留做法。	錄音腳本包括如何處理 Microsoft 個人數據，包括： ▪ 收集 ▪ 使用和 ▪ 保留

#	Microsoft 供應商數據保護要求	合規證明
	C 節： 選擇和同意	
8	在適用的情況下，供應商必須在收集數據主體的個人數據之前獲得並記錄數據主體對其所有處理活動（包括任何新的和更新的處理活動）的同意。 供應商監控偏好管理的有效性，以確保遵守偏好變更的時間框架是適用的最嚴格的當地法律要求。	供應商可以證明數據主體如何為處理活動提供同意，並且同意的範圍涵蓋供應商與該數據主體的個人數據相關的所有處理活動。 供應商可以證明數據主體如何撤回對處理活動的同意。 供應商可以演示在啟動新的處理活動之前如何檢查偏好。 備註： 證據可以是用戶交互截圖； 試用服務或查看技術文檔的機會。
9	創建和管理 Microsoft 網站和／或帶有 Microsoft 品牌的應用程序或網站的供應商必須根據 Microsoft 隱私聲明和當地法律要求中的承諾，向數據主體提供有關使用 Cookie 的透明通知和選擇。 除非簽約業務部門明確要求不這樣做，否則供應商應使用 1ES 生產的標準橫幅來管理選擇控制。 當網站針對歐盟／歐洲經濟區和其他適用隱私法的地區以及使用 Microsoft 隱私聲明的地方的用戶時，適用此要求。 備註： Microsoft 業務發起人需要在內部 Web 合規性門戶 (http://aka.ms/wcp) 中註冊 Microsoft 網站，以便對 Cookie 清單進行編目和管理。	必須記錄每個 Cookie 的用途，並且必須告知實施的 Cookie 類型。 若工作階段 Cookie 便足以使用時， ▪ 不得使用持久 Cookie。 ▪ 使用持久性 Cookie 時，它們的到期日期不得超過用戶訪問網站後 13 個月。 驗證是否符合適用的歐盟法律，例如： ▪ 使用標籤公約、隱私聲明中的「隱私和 Cookie」， ▪ 在將「非必要」Cookie 用於廣告等目的之前獲得明確的用户同意，以及 ▪ 同意必須會到期或每 6 個月內必須重新取得同意。

#	Microsoft 供應商數據保護要求	合規證明
	D 節： 收集	
10	供應商必須監控 Microsoft 個人和／或機密數據的收集，以確保僅收集執行所需的數據。	供應商可以提供證明需要收集的 Microsoft 個人和／或機密數據才能執行的文件。 供應商將應要求向 Microsoft 提供書面證據。
11	在從兒童（由適用的司法管轄區定義）收集數據之前，供應商必須根據當地隱私法律獲得同意。	供應商可以提供表明父母／監護人同意的文件。 供應商將應要求向 Microsoft 提供書面證據。
	E 節： 保留	
12	確保 Microsoft 個人和機密數據的保留時間不超過執行所需的時間，除非法律要求繼續保留 Microsoft 個人和／或機密數據。	供應商遵守 Microsoft 在合同中指定的書面保留政策或保留要求（例如，工作說明書、採購訂單）。 供應商將應要求向 Microsoft 提供書面證據。
13	確保由 Microsoft 自行決定，供應商擁有或控制的 Microsoft 個人和機密數據在履行完成後或應 Microsoft 的要求返回或銷毀。 在應用程序中，必須有適當的流程來確保當數據被用戶明確刪除或基於其他觸發條件（如數據壽命）從應用程序中刪除時，它能夠被安全地刪除。 當需要銷毀 Microsoft 個人或機密數據時，供應商必須燒毀、粉碎或切碎包含 Microsoft 個人和／或機密數據的實物資產，以確保無法讀取或重組信息。	保留 Microsoft 個人和機密數據的處置記錄（這可能包括交回 Microsoft 進行銷毀）。 如果 Microsoft 需要或要求銷毀，請提供由供應商官員簽署的銷毀證明。

#	Microsoft 供應商數據保護要求	合規證明
	F 節： 數據主體	
	數據主體根據法律享有某些權利，包括訪問、刪除、編輯、導出、限制和反對處理其個人數據的權利（「**數據主體權利**」）。 當數據主體尋求對其 Microsoft 個人數據行使法律規定的權利時，供應商必須允許 Microsoft 或者代表 Microsoft 執行以下操作：	
14	在可能的情況下，透過適當的技術和組織措施，協助 Microsoft 履行其義務，以響應數據主體尋求行使其數據主體權利的請求，不得無故拖延。 除非 Microsoft 另有指示，否則供應商會將直接聯繫供應商的所有數據主體推薦給 Microsoft 以行使他們的數據主體權利。	供應商將保留記錄流程和程序的證據，以支持數據主體權利的執行。 供應商將保留測試的書面證據。 可應 Microsoft 的要求提供證據。
15	當直接回複數據主體或供應商提供自助網上機制時，供應商有適當的流程和程序來識別提出請求的數據主體。	供應商已記錄用於識別 Microsoft 數據主體的方法。 供應商將應要求向 Microsoft 提供書面證據。
16	如果 Microsoft 要求查找無法透過自助在線機制獲得的有關數據主體的 Microsoft 個人數據，供應商將盡合理努力尋找所請求的數據並保留足夠的記錄以證明進行了合理的搜索。	供應商將保留程序的書面證據，以確定是否持有 Microsoft 個人數據，並將應要求向 Microsoft 提供文件。 供應商保留一份記錄，證明為滿足數據主體權利要求而採取的步驟。 文檔包括： ▪ 請求的日期和時間、 ▪ 為回應請求而採取的措施以及通知 Microsoft 的時間記錄。 供應商將應要求向 Microsoft 提供記錄保存的證據。

#	Microsoft 供應商數據保護要求	合規證明
	F 節： 數據主體（續）	
17	供應商將向數據主體傳達該人員必須採取的步驟，以獲取其 Microsoft 個人數據或以其他方式行使其權利。	供應商將保留有關存取 Microsoft 個人數據的通訊和程序的書面證據。 供應商將保留書面證據，並應要求向 Microsoft 提供相同的證據。
18	記錄數據主體權利請求的日期和時間以及供應商為回應此類請求而採取的行動。 如果他們的請求被拒絕，在 Microsoft 的指示下，向數據主體提供書面解釋。 根據要求向 Microsoft 提供數據主體請求的紀錄。	供應商保留存取／刪除請求的記錄，並記錄對 Microsoft 個人數據所做的更改。 記錄拒絕請求的實例並保留 Microsoft 審查和批准的證據。 供應商將提供記錄保存請求和拒絕存取 Microsoft 個人數據的證據。
19	供應商必須啟用 Microsoft 或以適當的印刷、電子或口頭格式為經過身份驗證的數據主體獲取所請求的 Microsoft 個人數據的副本。	供應商以數據主體和供應商易於理解的格式向數據主體提供 Microsoft 個人數據。
20	供應商必須採取合理的預防措施，以確保向 Microsoft 或經過身份驗證的數據主體發佈的 Microsoft 個人數據不能用於識別其他人。	供應商將保留與預防措施相關的程序的書面證據，以避免識別數據主體違反協議條款。 供應商將應要求向 Microsoft 提供證據。
21	如果數據主體認為其 Microsoft 個人數據不完整且不准確，則供應商必須將問題上報給 Microsoft，並在必要時與 Microsoft 合作解決問題。	供應商記錄分歧實例並將問題上報給 Microsoft。 供應商將應要求向 Microsoft 提供書面證據。

#	Microsoft 供應商數據保護要求	合規證明
	G 節： 分包商	
	如果供應商打算使用分包商來處理 Microsoft 個人或機密數據，則供應商必須：	
22	在分包服務或對添加或更換分包商進行任何更改之前通知 Microsoft。 備註： 表明您接受此義務，即使您目前沒有聘請分包商，但將來可能會這樣做。	驗證 Microsoft 個人數據僅由 Microsoft 根據適用合同（例如，工作說明書、附錄、採購訂單）要求或在 SSPA 數據庫中捕獲的公司處理。 供應商可以網上發佈其分包商列表，並在 SSPA 數據庫中包含指向該頁面的鏈接。
23	記錄由分包商分包處理的 Microsoft 個人和機密數據的性質和範圍，確保收集的訊息是執行所必需的。	供應商保留有關披露或轉移給分包商的 Microsoft 個人和機密數據的文檔。 供應商將應要求向 Microsoft 提供書面證據。
24	如果 Microsoft 是 Microsoft 個人數據的控制者，請確保分包商按數據主體聲明的聯繫偏好使用 Microsoft 個人數據。	展示分包商如何使用 Microsoft 數據主體首選項。 提供證明文檔（例如，畫面截圖、SLA、SOW 等），其中包括分包商遵守偏好更改的時間範圍。
25	將分包商對 Microsoft 個人或機密數據的處理限制為履行供應商與 Microsoft 的合同所必需的目的。	供應商可以提供文件，顯示需要向分包商提供給 Microsoft 個人數據才能執行。 供應商將應要求向 Microsoft 提供書面證據。
26	查看投訴是否有任何未經授權或非法處理 Microsoft 個人數據的跡象。	供應商可以證明系統和流程已到位，以解決有關分包商未經授權使用或披露 Microsoft 個人數據的投訴。 供應商將應要求向 Microsoft 提供書面證據。

#	Microsoft 供應商數據保護要求	合規證明
	G 節： 分包商（續）	
27	在得知分包商出於與績效相關以外的任何目的處理 Microsoft 個人或機密數據後，立即通知 Microsoft。	供應商已為分包商提供了報告濫用 Microsoft 數據的說明和方法。 供應商將應要求向 Microsoft 提供書面證據。
28	如果供應商代表 Microsoft 從第三方收集個人數據，則供應商必須驗證第三方數據保護政策和做法是否符合供應商與 Microsoft 和 DPR 的合同	供應商可以提供有關第三方數據保護政策和實踐的盡職調查文件。 供應商將應要求向 Microsoft 提供書面證據。
29	及時採取措施減輕因分包商未經授權或非法處理 Microsoft 個人和機密數據而造成的任何實際或潛在損害。	供應商必須保留計劃和程序的書面證據，並應要求向 Microsoft 提供文件證據。
	H 節： 質量	
30	供應商必須維護所有 Microsoft 個人數據的完整性，確保其準確、完整且與處理數據的既定目的相關。	供應商可以證明在收集、創建和更新 Microsoft 個人數據時已製定程序來驗證這些數據。 供應商可以證明已實施監控和抽樣程序，以持續驗證準確性並在必要時進行糾正。 供應商將應要求向 Microsoft 提供書面證據。

#	Microsoft 供應商數據保護要求	合規證明
	I 節： 監控和執行	
31	供應商制定了事件響應計劃，要求供應商在獲知數據事件後根據合同要求或不得無故拖延（以較早者為準）通知 Microsoft。 供應商必須根據 Microsoft 的要求或指示，與 Microsoft 合作對事件進行任何調查、緩解或補救，包括向 Microsoft 提供數據、訊息、對供應商人員的存取權限或進行取證審查所需的硬件。 備註： 請參閱 SSPA 計劃指南，了解如何將事件通知 Microsoft。	供應商有一個事件響應計劃，其中包括如本節所述通知客戶 (Microsoft) 的步驟。 供應商將應要求向 Microsoft 提供書面證據。
32	實施補救計劃並監控每個數據事件的解決方案，以確保及時採取適當的糾正措施	供應商已經記錄了應對數據事件以關閉的程序。 供應商將應要求向 Microsoft 提供書面證據。
33	如果 Microsoft 是 Microsoft 個人數據的控制者，請建立正式的投訴流程，以回應所有涉及 Microsoft 個人數據的數據保護投訴。	供應商有辦法接收涉及 Microsoft 個人數據的投訴，並有記錄在案的投訴程序來處理投訴。 供應商將應要求向 Microsoft 提供書面證據。

#	Microsoft 供應商數據保護要求	合規證明
	J 節： 安全性	
	供應商必須建立、實施和維護包括政策和程序在內的訊息安全計劃，以按照良好的行業慣例和法律要求保護和保持 Microsoft 個人和機密數據的安全。 供應商的安全計劃必須符合以下標準，要求 34 -50。	有效的 ISO 27001 認證可替代第 J 節目。聯繫 SSPA 以應用此替代品。 備註： 供應商將需要提供證明。
34	執行年度網絡安全評估，包括： ▪ 審查對環境的重大更改，例如新的系統組件、網絡拓撲、防火牆規則、 ▪ 進行漏洞掃描 ▪ 並維護更改日誌。	供應商已記錄網絡評估、更改日誌和掃描結果。 所需的更改日誌必須跟踪變化，提供有關更改原因的訊信息，並包括指定批准人的姓名和職務。
35	供應商定義、傳達和實施移動設備策略，以保護和限制在移動設備上存取或使用的 Microsoft 個人或機密數據的使用。	在 Microsoft 個人或機密數據處理需要使用移動設備的情況下，供應商證明使用了合規的移動設備政策。
36	用於支持績效的所有資產都必須進行核算並具有確定的所有者。 供應商負責維護這些信息資產的清單；確定資產的可接受和授權使用； 並在資產的整個生命週期內為其提供適當水平的保護。	用於支持性能的設備資產清單。 這些資產的清單，包括以及不再需要數據存儲介質時的處置記錄： ▪ 設備的位置、 ▪ 資產數據的數據分類、 ▪ 終止僱傭或業務協議時的資產回收紀錄， ▪ 以及不再需要數據存儲介質時的處置紀錄。

#	Microsoft 供應商數據保護要求	合規證明
	J 節： 安全性（續）	
37	建立並維護訪問權限管理程序，以防止未經授權訪問供應商控制下的任何 Microsoft 個人或機密數據。	供應商證明其已實施訪問權限管理計劃，其中包括以及： ▪ 訪問控製程序、 ▪ 識別程序、 ▪ 失敗後的鎖定程序、 ▪ 用於選擇身份驗證憑據的穩健參數，以及 ▪ 在 僱傭關係終止時48 小時內停用用戶帳戶 ▪ 加強密碼控制，強制密碼長度和復雜性並防止重複使用 供應商證明其具有審查用戶對 Microsoft 個人和機密數據的訪問權限的既定流程，以執行最小權限原則。該過程包括 ▪ 明確定義的用戶角色、 ▪ 審查和證明對角色訪問權限的批准的程序， ▪ 以及測試角色內有權訪問 Microsoft 數據的用戶是否有文件證明屬於該組／角色。
38	定義和實施補丁管理程序，優先處理用於處理 Microsoft 個人或機密數據的系統的安全補丁。 這些程序包括： ▪ 確定安全補丁優先級的風險方法 ▪ 處理和實施緊急補丁的能力、 ▪ 適用於操作系統和服務器軟件（例如應用程序服務器和數據庫軟件）、 ▪ 記錄補丁緩解的風險並跟踪任何異常情況，以及， ▪ 要求授權公司不再支持的軟件進行退役。	供應商可以展示滿足此要求並至少涵蓋以下內容的已實施補丁管理程序。 ▪ 分配嚴重性以通知優先級。（記錄嚴重性定義。） ▪ 實施緊急補丁的記錄程序。 ▪ 驗證，不再使用創作公司不再支持的操作系統。 ▪ 跟踪批准和異常的補丁管理記錄。

#	Microsoft 供應商數據保護要求	合規證明
	J 節： 安全性（續）	
39	在用於處理 Microsoft 個人和機密數據的聯網設備（包括服務器、生產和培訓桌面）上安裝防病毒和反惡意軟件，以阻止潛在的有害病毒和惡意軟件應用程序。 每天或按照防病毒／反惡意軟件供應商的指示更新反惡意軟件定義。 備註： 這適用於包括 Linux 在內的所有操作系統。	存在記錄以顯示防病毒和反惡意軟件的使用處於活動狀態。 備註： 此要求適用於所有操作系統。
40	為 Microsoft 開發軟件的供應商必須在構建過程中納入安全設計原則。	供應商技術規範文件包括其開發週期中的安全驗證檢查點。
41	採用數據丟失防護（「**DLP**」）程序來防止入侵、丟失和其他未經授權的活動。必須對數據進行適當分類、標記和保護，並且供應商必須監控在處理 Microsoft 個人或機密數據時使用的資訊系統是否存在入侵、丟失和其他未經授權的活動。 如果您保留 Microsoft 個人或機密數據，DLP 程序至少： ▪ 需要使用行業標準主機、網絡和基於雲的入侵檢測系統（「**IDS**」）， ▪ 需要實施高級入侵保護系統（「**IPS**」）配置為監控並主動阻止數據丟失， ▪ 如果系統遭到破壞，需要對系統進行分析以確保還解決任何殘留的漏洞， ▪ 描述監控系統危害檢測工具所需的程序， ▪ 檢測到數據事件時，建立需要執行的事件響應和管理流程，， ▪ 並要求就未經授權下載和使用 Microsoft 個人或機密數據與所有供應商員工和被從供應商績效中分離出來的分包商進行通信）。	已部署的文檔化 DLP 程序，並採用適當的程序來防止入侵、丟失和其他未經授權的活動（至少，本節中指定的所有項目）。

#	Microsoft 供應商數據保護要求	合規證明
	J 節： 安全性（續）	
42	及時將事件響應的調查結果傳達給高級管理層和 Microsoft。	系統和流程必須到位，以便將事件響應調查結果傳達給 Microsoft。
43	系統管理員、操作人員、管理層和第三方必須接受年度安全培訓。	建立安全培訓計劃，包括： ▪ 事件響應年度培訓、 ▪ 模擬事件和自動化機制，以促進對危機情況的有效響應。 ▪ 事件預防意識，例如與下載惡意軟件相關的風險。
44	供應商必須確保備份計劃流程保護 Microsoft 個人和機密數據免遭未經授權的使用、訪問、披露、更改和破壞。	供應商可以展示書面回應和恢復程序，詳細說明組織將如何管理破壞性事件，並將其訊息安全維持在基於管理層批准的訊息安全連續性目標的預定水平。 供應商可以證明其已定義並實施了定期備份、安全存儲和有效恢復關鍵數據的程序。
45	建立和測試業務連續性和災難恢復計劃	災難恢復計劃必須包括以下內容： ▪ 確定係統是否對供應商業務運營至關重要的定義標準。 ▪ 根據定義的標準列出在發生災難時必須作為恢復目標的關鍵系統。 ▪ 為每個關鍵系統定義災難恢復程序，確保不了解系統的工程師可以在 72 小時內恢復應用程序。 ▪ 每年（或更頻繁地）測試和審查災難恢復計劃，以確保能夠滿足恢復目標。

#	Microsoft 供應商數據保護要求	合規證明
	J 節： 安全性（續）	
46	在授予個人訪問 Microsoft 個人或機密數據的權限之前驗證個人的身份，並確保訪問權限僅限於特定個人允許支持性能的活動範圍。	確保所有用戶 ID 都是唯一的，並且每個用戶 ID 都具有行業標準的身份驗證方法，例如 Azure Active Directory。 提升存取權限（管理或其他類型的增強權限）必須使用第二個因素，例如智能卡或基於電話的身份驗證器。 記錄的訊息安全計劃涵蓋確保所有供應商員工和分包商訪問 Microsoft 個人或機密數據的過程不超過或超過支持績效所需的時間。
47	供應商必須透過使用傳輸層安全性（「**TLS**」）或互聯網協議安全性（「**IPsec**」）的加密來保護與其性能相關的所有處理過的數據。 這些方法在 NIST 800-52 和 NIST 800-57 中有所描述； 也可以使用等效的行業標準。 供應商必須拒絕交付透過未加密方式傳輸的任何 Microsoft 個人或機密數據。	必須定義和執行創建、部署和替換 TLS 或其他證書的過程。
48	所有將訪問或處理 Microsoft 個人或機密數據的供應商設備（筆記本電腦、工作站等）都必須採用基於磁盤的加密。	加密所有設備以滿足用於處理 Microsoft 個人或機密數據的所有客戶端設備的 BitLocker 或其他行業等效磁盤加密解決方案。

#	Microsoft 供應商數據保護要求	合規證明
	J 節： 安全性（續）	
49	系統和程序（使用當前行業標準，例如 **NIST 800-111** 標準中描述的標準）必須到位，以在靜態（存儲時）加密任何和所有 Microsoft 個人和／或機密數據，示例包括但不限於： ▪ 憑證數據（例如，用戶名／密碼） ▪ 付款工具資料（例如，信用卡和銀行戶口號碼） ▪ 移民相關的個人資料 ▪ 醫療檔案數據（例如，用於身份驗證的醫療記錄編號或生物特徵標記或標識符，例如 DNA、指紋、眼睛視網膜和虹膜、語音模式、面部模式和手部測量值） ▪ 政府簽發的標識符數據（例如，社會保障或駕駛執照號碼） ▪ 屬於 Microsoft 客戶的數據（例如 SharePoint、O365 文檔、OneDrive 客戶） ▪ 與未發佈的 Microsoft 產品相關的材料 ▪ 出生日期 ▪ 孩子的個人資料 ▪ 實時地理數據 ▪ 實際個人（非商業）地址 ▪ 個人（非商業）電話號碼 ▪ 宗教 ▪ 政見 ▪ 性取向／偏好 ▪ 安全問題答案（例如，2fa、密碼重置） ▪ 母親的娘家姓氏	檢查 Microsoft 個人和機密數據是否在靜態時加密。
50	匿名化開發或測試環境中使用到的所有 Microsoft 個人數據。	不得在開發或測試環境中使用 Microsoft 個人數據；當別無選擇時，必須將其匿名化，以防止識別數據主體或濫用個人數據。 備註： 匿名數據不同於假名數據。 匿名數據是與已識別或可識別的自然人無關的數據，其中個人數據的數據主體不可識別或不再可識別。

「**授權代表**」是具有適當級別授權代表公司簽字的人。 此人應具備必要的隱私和安全知識，或在提交對 SSPA 計劃行動的回應之前諮詢過主題專家。 此外，透過將他們的姓名添加到 SSPA 表格中，他們證明他們已閱讀並理解 DPR。

「**EUDPR**」是指歐洲議會和理事會於 2018 年 10 月 23 日頒布的第 (EU) 2018/1725 號條例，關於在歐盟機構、團體、辦事處和機構處理個人數據方面保護自然人，以及 此類數據的自由流動，並廢除第 45/2001 號條例 (EC) 和第 1247/2002/EC 號決定。

「**自由職業者**」是指執行按需任務或服務的個人，這些任務或服務是透過數字平台或其他方式採購的。

「**GDPR**」指 2016 年 4 月 27 日歐洲議會和理事會關於在處理個人數據和此類數據的自由流動方面保護自然人的條例 (EU) 2016/679，並廢除指令 95/46/ EC（通用數據保護條例）。

「**隱私數據保護要求**」是指 GDPR、EUDPR、當地 EU/EEA 數據保護法、加利福尼亞州消費者隱私法。 民法典 § 1798.100 及以下。 （「*CCPA*」）、2018 年英國數據保護法和適用於英國的任何相關或後續法律、法規和其他法律要求，以及與 (a) 隱私和數據安全相關的任何適用法律、法規和其他法律要求；(b) 任何個人數據的使用、收集、保留、存儲、安全、披露、轉移、處置和其他處理。

「歐盟示範條款」和「標準合同條款」是指 (i) 標準數據保護條款，用於將個人數據傳輸給在第三國設立的處理者，這些條款不能確保充分的數據保護水平，如歐盟第 46 條所述 GDPR 並經歐盟委員會 2021 年 6 月 4 日第 (EU) 2021/914 號決定批准；(ii) (a) 歐盟委員會、(b) 歐洲數據保護監管機構透過並經歐盟委員會批准、(c) 英國根據英國《通用聯邦數據保護法》採用的任何後續標準合同條款，(d) 瑞士根據《瑞士聯邦數據保護法》，或 (e) 由瑞士、英國和歐盟/歐洲經濟區組成的司法管轄區以外的管轄區的政府執行，這些條款管轄個人數據的國際傳輸，應自其採用之日起納入並對供應商具有約束力。

「網站託管」網站託管服務是一種網上服務，它代表 Microsoft 在 Microsoft 域下創建和/或維護網站，即供應商提供創建和維護網站所需的所有材料和服務，並使其可在 互聯網。「網絡託管服務提供商」或「網絡託管商」是指提供網站或網頁在互聯網上瀏覽所需的工具和服務的供應商，例如用於廣告的 Cookie 或網絡信標。