PayPal

>> 檢視所有同意書

PayPal 卡片付款處理產品的資料保護附錄

最近更新日期：2021 年 12 月 1 日

本 PayPal 卡片付款處理產品的資料保護附錄（簡稱本「附錄」）適用於任何 PayPal 集團成員（簡稱「PayPal」）向你、商店（簡稱「商店」或「你」）提供卡片付款處理服務、金流閘道服務及 / 或預防詐騙服務（簡稱「付款服務」）的任何產品、服務或其他服務。本附錄不適用於 PayPal 錢包服務，例如：使用 PayPal 付款或 PayPal 的 Pay Later 優惠活動。本附錄構成商店與 PayPal 之間相關同意書的一部分，並以引用方式納入其中，該同意書規範 PayPal 向你提供的付款服務（簡稱「同意書」）的條款。若本附錄的條款與同意書之間存在任何衝突，應以本附錄的條款為準。本附錄中使用但未定義的大寫術語，應具有同意書所述之含義。

本附錄自 (i) 同意書所指明的生效日期，或 (ii) 向你發佈或提供的本附錄相關通知中所載生效日期起生效，以較晚者為準。我們可能會不定時修訂本附錄。除非另有說明，否則修訂版本將自發佈於我們的網站時即時生效。如果我們的變更會縮減你的權利或增加你的責任，我們將在本同意書要求的期限內，於網站的「政策更新」頁面上發佈通知。如果你不同意對本附錄所做的任何變更，你可以停止使用付款服務。

定義

下列術語在本「附錄」使用時的含義如下：

「**控制者**」意指*決定處理「個人資料」用途和方式的實體，或者，如果「資料保護法」已定義此類術語（或表示類似功能的術語），則「控制者」應具有適用「資料保護法」所界定的含義。*

「**客戶**」意指使用「付款服務」的客戶，就本附錄而言，他們為資料主體。

「**客戶資料**」意指 (i) 客戶提供給商店，而商店透過使用付款服務傳送給 PayPal 的個人資料，以及 (ii) PayPal 可透過商店使用付款服務收集到的客戶裝置及瀏覽器資料。

「**資料保護法**」意指適用於提供付款服務的資料保護法律、法規、法令、監管規定及業務守則，包括任何相關修訂與任何相關的法規或工具（例如，2018 年《加州消費者隱私保護法》、《加州民法》第 1798.100 條以降、歐盟第 2016/679 號規則《一般資料保護規範》(GDPR)、《澳洲 1988 年隱私權法案》(Cth)、《個人資料保護及電子文件法》（加拿大）、《個人資料（私隱）條例》（第 486 章）（香港）、《巴西一般資料保護法》、聯邦法第13709/2018 號與 2012 年《個人資料保護法》（新加坡）。

「PayPal 集團」意指 PayPal, Inc. 及 PayPal 或其後繼公司直接或間接不定時持有或控制的所有公司。

「**個人資料**」意指與已識別或可識別自然人（「資料主體」）相關的任何資訊；所謂可識別的自然人，意指可以直接或間接，特別是透過涉及如姓名、身分證號碼、居住資料、線上識別碼的識別資料，或是一個或多個身體、生理、遺傳、心理、經濟、文化或社會身分等特定因素而可識別的自然人。

本附錄使用表示類似功能的「**處理程序**」或術語，應具有適用「資料保護法」中定義的含義。

PayPal 為控制者

PayPal 應遵守本附錄關於處理客戶資料中，適用於控制者的資料保護法規定（包括但不限於在任何時候實施並維護所有與處理客戶資料相關的適當安全措施），且不得故意進行或允許進行，任何有可能導致商店違反資料保護法的客戶資料相關行為。PayPal 僅可將客戶資料轉移給第三方、分包處理者或 PayPal 集團成員，且其應簽訂包含客戶資料保護條款的書面同意書，且其保護程度不亞於本附錄中所述的條款。

處理與付款服務相關的客戶資料

雙方瞭解並同意，商店及 PayPal 是各自獨立的「控制者」，處理與付款服務相關的所有客戶資料。因此，PayPal 獨立決定處理該等客戶資料的目的和方式，並非與商店為該等客戶資料的共同控制者。

雙方瞭解並同意，PayPal 獲准為以下有限目的使用、複製和處理客戶資料及付款交易資料:

- 為商店與其客戶提供並改善付款服務的合理需求，包括預防詐騙工具；
- 監控、預防與偵測詐騙性付款交易，並防止對商店、PayPal 及第三方造成損害；

- 遵守適用於 PayPal 處理及保留付款資料的法律或監管責任，包括適用的防洗錢及身分認證責任；
- 分析、開發並改善 PayPal 的產品與服務；
- 內部使用，包括但不限於資料分析與指標；
- 以無法識別你的個人或用戶客戶資料的彙總方式，彙整並披露客戶資料及付款交易資料，包括按地區或產業計算你的平均值；
- 遵守適用的法律規定，並依法回應披露資料的要求以協助執法機關；以及
- 如有任何其他用途，只要該用途符合資料保護法，便會通知商店。

商店通知客戶

商店應使用商業上合理的努力 (i) 在隱私權政策中告知客戶，PayPal 為本附錄所述處理客戶資料的獨立控制者，並在 (ii) 商店的隱私權政策中加入 www.paypal.com 網站上的 PayPal 隱私權聲明連結。

互助

雙方同意在合理必要的範圍內彼此合作，以使另一方能夠根據資料保護法，充分履行其作為獨立控制者的責任。雙方同意，根據資料保護法，商店收到資料主體存取請求或客戶行使其權利時，商店應直接回應此客戶的存取請求。商店也應告知客戶，他們可根據 **www.paypal.com** 網站上《隱私權聲明》所述的指示，以行使其與 PayPal 付款服務相關的資料主體權利。此外，如果與任何交易安全事件有關，PayPal 自行決定必須通知受影響的客戶，而 PayPal 並沒有關於受影響客戶的必要聯絡資料來進行此類溝通，則商店應使用商業上合理的努力，向 PayPal 提供商店可能擁有的客戶相關資料，滿足 PayPal 為遵守資料保護法有關受影響客戶所適用之通知責任的有限目的。

跨境資料傳輸

雙方同意，PayPal 得在提供付款服務所需的情況下，將根據本同意書處理的客戶資料傳輸至收集資料國家以外的區域。如果 PayPal 將本附錄所保護的客戶資料傳輸至一司法管轄區，而該司法管轄區未取得收集資料所在國家主管機關通過的適足性認定，PayPal 將確保根據適用的資料保護法，為客戶資料的傳輸實施適當的保障措施。例如，基於遵守《一般資料保護規範》(GDPR) 之目的，我們仰賴主管機關批准的《拘束性企業規則》及其他資料傳輸機制，將客戶資料傳輸至其他 PayPal 集團成員。

針對你將位於歐盟、瑞士、歐洲經濟區和 / 或其成員國或英國的客戶資料傳輸至 PayPal，我們皆同意 (i) 在適用的範圍內，你簽署此同意書後，即視為商店作為資料匯出方及控制者簽署並接受歐盟執委會於 2021 年 6 月 4 日以歐盟第 2021/914 號決議發布，有關根據《一般資料保護規範》(GDPR) 將個人資料傳輸至第三國之標

準契約條款（簡稱「歐盟傳輸條款」）；並作為資料匯出方簽署並接受內閣大臣依據 2018 年《資料保護法》第 17C(b) 條制定且現行適用於英國之法規中指定的標準資料保護條款（簡稱「英國傳輸條款」），以及 (ii) 在適用的範圍內，PayPal 簽署同意書後，即視為 PayPal 作為資料匯入方及控制者簽署並接受歐盟傳輸條款；並作為資料匯入方簽署並接受英國傳輸條款，且 (iii) 雙方應遵守歐盟傳輸條款之模組 1 的規定。若歐盟執委會 / 英國內閣大臣（或其他適用的英國授權機構）分別修改並隨後發佈新版歐盟傳輸條款 / 英國傳輸條款，或歐盟執委會 / 英國內閣大臣（或其他適用的英國授權機構）另行提出要求或實施，則雙方同意新版歐盟傳輸條款 / 英國傳輸條款（如適用）將取代目前的歐盟傳輸條款 / 英國傳輸條款，且雙方同意採取一切必要行動，以使新版歐盟傳輸條款 / 英國傳輸條款實施生效（如適用）。歐盟傳輸條款（模組 1）及英國傳輸條款將透過引用的方式納入本同意書，並在此同意書生效時被視為在雙方之間正式執行，但需遵循以下細節：

A) 歐盟傳輸條款

1. 應以第 17 條第 1 項（準據法）為準，且歐盟條款應受盧森堡法律管轄；
2. 根據第 18 條（合意選擇法院與司法管轄權），盧森堡法院將解決任何因歐盟條款產生的糾紛申訴；以及
3. 雙方皆同意歐盟傳輸條款附錄所要求的詳細資訊，如附件 1 所載。

B) 英國傳輸條款

1. 已併入第 II(h)(iii) 條款，PayPal 簽署此同意書後，即視為 PayPal 作為資料匯入方的必要縮寫簽名；
2. 雙方皆同意英國傳輸條款附件 B 所要求的詳細資訊，如附件 1 所載（在適用的範圍內）。

<u>附件 1</u>

歐盟傳輸條款附錄與英國傳輸條款附件 B

A) 在所需的範圍內，以下內容適用於歐盟傳輸條款與英國傳輸條款

附件 1.A. 締約方名單

資料匯出方

- 姓名和地址：資料匯出方為商店，地址如本同意書所列
- 聯絡人姓名、職位和詳細聯絡資料：如本同意書所列
- 根據標準契約條款傳輸之資料相關的活動：如本同意書所列
- 簽名與日期：請參閱本附錄中「跨境傳輸」一節

- 角色（控制者 / 處理者）：控制者

資料匯入方

- 姓名和地址：資料匯入方為根據本同意書提供服務的 PayPal 集團成員，地址如本同意書所列
- 聯絡人姓名、職位和詳細聯絡資料：如本同意書所列
- 根據標準契約條款傳輸之資料相關的活動：如本同意書所列 簽名與日期：請參閱本附錄中「跨境傳輸」一節
- 角色（控制者 / 處理者）：控制者

附件 1.B.傳輸說明

資料主體
傳輸的個人資料涉及以下資料主體類型:

資料匯出方及其客戶、員工和其他業務聯絡人。

傳輸的個人資料類型

傳輸的個人資料可能包括以下資料類型:

姓名、收費金額、日期 / 時間、銀行帳戶詳細資料、付款信用卡詳細資料、信用卡驗證碼 (CVC)、郵遞區號、國家 / 地區代碼、地址、電子郵件地址、傳真、電話號碼、網站、有效期限、運送詳細資料、納稅身分、唯一客戶識別碼、IP 位址、地點，以及 PayPal 根據此同意書所取得的任何其他資料。

敏感性資料（如適用）與適用限制或保障措施

傳輸的個人資料涉及下列類型的敏感性資料:

- 不適用，除非商店設定該服務以取得此類資料。
- 適用限制和保障措施:
- 不適用，除非商店設定該服務以取得此類資料。

處理性質

- 如本同意書中所述。

傳輸目的
資料傳輸目的如下:

- 資料匯入方遵照此同意書，向資料匯出方履行其所提供的服務。
- 識別會影響或可能影響資料匯入方、資料匯出方或資料匯入方其他客戶的詐騙活動與風險。
- 遵守適用於資料匯入方的法律。
- 如資料保護附錄中所述。

個人資料將被保留的期限，若不適用，則提供用於決定期限的標準

資料匯入方僅於收集個人資料相關目的所需的時間內保留該個人資料（請參閱上述目的）。為了確定適當的個人資料保留期限，資料匯入方會考慮個人資料的數量、性質和敏感性、未授權使用或披露個人資料的潛在損害風險、處理個人資料的目的以及該等目的是否可透過其他方式實現，以及適用法律、法規、稅務、會計或其他要求。

傳輸至（分包）處理者，並說明處理的主題、性質和期限

資料匯入方可能會與依據資料匯入方指示，並代表其執行服務和功能的第三方服務供應商分享個人資料。這些第三方服務供應商可能會提供本同意書規定提供服務之元素（例如客戶認證、交易處理或客戶服務），或向資料匯入方提供服務，以支援本同意書規定提供的服務（例如儲存）。決定第三方服務供應商進行處理的期限時，資料匯入方應採用本附件 1.B 中的上述標準。

附件 1.C.監管機關

根據歐盟傳輸條款第 13(a) 條，負責確保資料匯出方遵守歐盟第 2016/679 規則進行資料傳輸的監管機關（如所示），應擔任主管機關。

附件 II.技術和組織措施，包括確保資料安全的技術和組織措施

1. 虛擬假名、加密和傳輸時的資料保護

PayPal 的政策確保遵守此原則，並要求使用技術管制以預防披露個人資料的風險。PayPal 對所有個人資料採用傳輸中加密和靜態加密。我們同樣採用業界標準的虛擬假名技術，例如在適用的情況下以標記化來保護個人資料。PayPal 擁有完善的政策，提供關鍵義務與流程，以保護在企業內部和外部與第三方之間傳輸的資料。

2. 變更管理與營運持續。

PayPal 的健全變更管理流程透過確保變更得到適當的規劃、核准、執行和審查，在整個生命週期內保護資料和系統的持續可用性和彈性。公司的營運持續管理流程

為建立組織韌性提供了一個框架，具有有效回應的能力，可保障重要關係人的利益。

3. 災害復原。

PayPal 的健全災害復原方案設有在任何嚴重中斷情況下復原資料系統或技術系統的流程，主要針對支援關鍵業務流程與客戶活動的 IT 系統。PayPal 技術基礎架構設於多個安全資料中心，具有主要和次要功能，均配有網路和安全基礎架構、專屬應用程式、資料庫伺服器和儲存裝置。

4. 定期測試、評估和評量技術與組織措施的效能。

PayPal 定期規劃、執行和報告公司的測試方案結果，以評估和評量其技術與組織措施的效能。該方案由我們的企業風險與法規遵循團隊管理，他們與相關的關係人合作，以獲得並評量進行必要測試、報告和補救時所需的資訊。

5. 用戶身分識別與授權。

PayPal 存取管理流程要求用戶在存取任何其他範圍內應用程式前，使用專屬的企業網路帳戶 ID 和密碼登入企業網路，進行用戶身分識別與驗證。自動適用密碼組成、長度、變更、重複使用和鎖定的相關政策。在所有範圍內的系統中實施角色型存取與核准，每季度進行一次認證，以執行最小特權原則。

6. 處理個人資料地點的實體安全。

PayPal 全球安全和交易安全政策與流程根據適用法律、法規和合作夥伴需求規定了必需的要求，以促進健全的安全和交易安全流程，包括實體交易安全。根據公司的資訊安全處理標準，在建造郵件收發室、器材存放、運送和接收區、電腦 / 伺服器室、通訊保管庫或機密文件 / 資訊儲存區等特殊或敏感性區域時，特別重視交易安全系統和保障措施。

7. 事件記錄與設定。

PayPal 已概述並定義事件記錄和監控類型與屬性。公司會收集並彙總數種記錄檔類型至集中安全監控系統。啟用標準設定管理控制，確保從系統中收集記錄檔，然後轉至我們的集中安全監控系統。PayPal 政策和支援流程規定，所有系統均需實施系統設定和強化基準。

8. IT 治理與管理；流程和產品的認證與保證。

PayPal 在全公司內推廣健全的交易安全理念。我們的資安長負責監督我們全球企業的資訊交易安全。作為我們企業風險與法規遵循管理方案的一部分，我們的技術監督與資訊交易安全方案旨在協助公司管理技術和資訊交易安全風險，並識別、保護、偵測、回應資訊交易安全威脅並從中恢復。PayPal 透過各種各業方案認證及保證其流程與產品，包括 (i) 對 PayPal 技術產業標準義務的稽核與評估，包括但不限於 ISO 27001、支付卡產業 (PCI) 適用標準（DSS、PIN、P2PE 等）和美國註冊會計師協會 (AICPA) SOC-1 和 SOC-2；(ii) 風險控制識別流程 (RCIP)，確保早期參與，並以標準方法測量、管理和監控與產品解決方案的開發與發佈相關的風險；(iii) 隱私衝擊評估，納入產品和軟體開發流程初期階段，以及 (iv) 全面的第三方管理方案，透過在與第三方合作的生命週期內持續的風險管理來提供保證。

9. 資料最小化。

我們的政策要求，透過技術管制，收集和生成的資料元素是那些充分、相關並限於與處理目的相關的必要內容。PayPal 隱私衝擊評估流程確保遵守這些政策。

10. 資料品質與保存。

PayPal 存取與品質政策確保所有個人資料均正確、完整並且為最新狀態，使個人用戶能夠存取系統以修正並變更特定資料（例如地址、詳細聯絡資料等），並在收到資料主體的修正要求時，提供履行其修正權的服務。我們的資料治理方案會在必要時監控資料品質、問題和補救措施。根據 PayPal 的法律、法規和營運紀錄保存要求，我們要求所有資料均依據其商業價值進行分類，並指定保留期限。保留期限屆滿時，資料和資訊將被清除、刪除或銷毀。

11. 當責。

PayPal 開發一套符合業界標準的資訊交易安全、技術、資料治理、第三方管理和隱私權政策及原則，旨在讓關係人協作與合夥經營，使整個組織了解並遵守這些政策和控制措施，以確保整個組織自上而下的參與和當責。每個方案都定義了跨功能資訊的相關決策、流程和控制決策的責任。作為資料控制者，PayPal 負責並證明遵守《一般資料保護規範》(GDPR) 和其他適用資料保護法中具有當責義務的相關條款，透過實施隱私權方案政策和基本分層組織與技術控制結構，以確保整個企業遵循法律、法規、政策和流程。這包括能透過以下方式證明對資料保護法的遵守：1) 深厚的守法文化；2) 企業風險與法規遵循治理結構，包括管理委員會、監督角色、隱私權報告；3) 企業機能對遵守隱私權方案的責任，包括建立、記錄和維護業務流程與控制措施；4) 企業法規遵循組織內的全球隱私權部門，監督企業對隱私權方案的遵守情況，並定義由企業機能部門進行操作的政策、標準、流程和工具；5) 全球隱私權部門與企業通訊，以促進對隱私權的認識和了解；6) 企業風險與法規遵循管理框架，以確保採用一致的流程，包括隱私衝擊評估、隱私監控與測

試、隱私問題管理、隱私培訓、年度隱私權方案，以及 7) 向監督隱私權方案的管理委員會進行報告與分析。

12. 資料主體之權利。

PayPal 設有方案，用於確保資料主體的權利得以履行，包括存取、修正和清除。除非 PayPal 具有法律、法規義務或其他正當業務理由保留資料，否則將履行資料清除的要求。PayPal 政策確保資料清除在整個客戶生命週期內進行。

13. 處理者。

PayPal 設有完善的第三方管理方案，透過在與第三方合作的整個生命週期內持續管理風險來提供保證。我們有契約控制措施，要求我們的處理者與其分包處理者在整個程序鏈中制定全面的資料交易安全和隱私權標準。所有分包處理者都必須在參與前取得我們的預先核准。

B) 以下內容僅適用於英國傳輸條款

資料接收者
傳輸的個人資料僅能向以下資料接收者揭露：

- 匯入方的服務提供者、關係企業，以及根據此同意書執行服務的相關人員。

資料匯出方的資料保護註冊資訊（若適用）

不適用。

其他實用資訊（儲存限額和其他相關資訊）

如本同意書和本附件 1 前文中所述。