

[PayPal](#)

>> [查看所有法律同意書](#)

PayPal 信用卡和扣帳卡付款處理產品之資料保障增編

 [列印](#)

最後更新日期：2021 年 12 月 1 日

本 PayPal 信用卡和扣帳卡付款處理產品之資料保障增編（下稱「增編」）適用於任何產品、服務或其他由 PayPal 集團（下稱「PayPal」）成員向你這位商家（下稱「商家」或「你」）提供的信用卡和扣帳卡付款處理、闡道及 / 或預防欺詐服務（下稱「付款服務」）。本增編不適用於 PayPal 錢包服務，例如 PayPal 安全支付或 PayPal 稍後付款服務。本增編應構成商家與 PayPal 之間相關同意書（下稱「同意書」）的一部分，規管 PayPal 向你提供的付款服務，並以提述的方式納入同意書中。若本增編與同意書的條款之間存在任何衝突，應以本增編的條款為準。本增編使用的詞彙如無定義，則其含意應與同意書上所載的定義一致。

本增編的生效日期為 (i) 自同意書中列明的生效日期起計，或 (ii) 自我們就本增編向你發佈或提供的通知中列明之生效日期起計，以較晚者為準。我們可以不時修改本增編。除非另有說明，否則經修改的版本將會在我們發佈於網站時生效。若我們的變更導致你的權利有所減少或你的責任有所增加，我們會按照同意書規定的時限內在網站的「[政策更新](#)」頁面中發佈通知。若你不同意本增編的任何變更，你可以終止使用付款服務。

定義

以下詞彙在本增編中使用時定義如下：

「**控制方**」是指一個實體，此實體決定處理個人資料的目的及方式；如果資料保障法中對此詞彙（或指涉類似作用的詞彙）有所定義時，「控制方」則應採用適用資料保障法所定義的含義。

「**客戶**」是指使用付款服務的客戶，在本增編當中，他們屬於資料主體。

「**客戶資料**」是指 (i) 客戶向商家提供的個人資料，而商家透過其使用的付款服務將之傳送給 PayPal，和 (ii) PayPal 透過商家使用的付款服務，從客戶的裝置及瀏覽器中收集的個人資料。

「**資料保障法**」是指適用於提供付款服務的任何適用資料保障法律、法規、指令、監管要求及行為守則，包括其中的任何修訂及任何相關法規或文件（例如《2018年加州消費者私隱法案》（加州民法第 1798.100 條及其後各條）、《一般資料保障條例》（歐盟法規編號：2016/679，簡稱 GDPR）、《1988年澳洲私隱法案》（Cth）、《個人資料保護和電子文件法案》（加拿大）、《個人資料（私隱）條例》（香港法例第 486 章）《巴西一般資料保護法》（聯邦法律第13,709/2018 號）及《2012年個人資料保護法》（新加坡））。

「**PayPal 集團**」是指 PayPal, Inc. 及 PayPal 或其繼任者直接或間接不時擁有或控制的所有公司。

「**個人資料**」指與已識別或可識別自然人（即「資料主體」）相關的任何資料；可識別自然人是指可直接或間接識別的自然人，尤其是指可透過以下資料識別的自然人，例如：姓名、身份證號碼、位置資料、網上識別碼，或者專屬於此自然人的身體、心理、基因、精神、經濟、文化或社會身份等特定的一個或多個因素。

在本增編中使用的「**流程**」或具有類似含義的詞彙，均應採用適用資料保障法所定義的含義。

PayPal 作為資料控制方

根據本增編，PayPal 在處理客戶資料時應遵守適用於控制方的資料保障法要求（包括但不限於：在處理客戶資料方面，始終實行並維持所有適當的安全措施），且不得在知情的情況下，就客戶資料作出或允許可能導致商家違反資料保障法的行為。若 PayPal 向第三方、子處理商或 PayPal 集團成員傳送客戶資料，則必須與該等第三方、子處理商或 PayPal 集團成員訂立包含客戶資料保障條款的書面同意書，且該等同意書的保障力度不得低於本增編所列條款。

處理與付款服務相關的客戶資料

各方確認並同意，在與付款服務有關的所有客戶資料處理事宜上，商家及 PayPal 均為獨立的控制方。因此，PayPal 將獨立決定處理此等客戶資料的目的及方式，並且不會與商家共同構成此等客戶資料的聯合控制方。

各方確認並同意，PayPal 可以出於以下有限目的來使用、複製及處理客戶資料和付款交易資料：

- 在有合理需要時，提供及改善為商家及其客戶而設的付款服務，包括預防欺詐工具；
- 監察、預防及偵測欺詐性付款交易，並防止對商家、PayPal 及第三方造成損害；
- 遵守適用於付款資料處理及保留，且 PayPal 需受其約束的法律或監管義務，包括適用的反洗黑錢及身份核實義務；
- 分析、研發及改善 PayPal 的產品和服務；
- 內部使用，包括但不限於資料分析及數據衡量；
- 彙編和披露無法識別個人或用戶客戶資料的綜合客戶數據和付款交易資料，包括按區域或行業計算平均值；
- 根據法律規定回覆有關資料披露之請求，以便遵守適用法律要求並協助執法機構；及
- 有向商家通知的任何其他目的，惟該等目的必須符合資料保障法。

商家向客戶發出的通知

商家應採用商業上合理的方式，(i) 於其私隱權聲明中通知客戶，指出 PayPal 在處理客戶資料上為獨立控制方，如本增編所述；並且 (ii) 於其商家私隱權聲明中加入 PayPal 私隱權聲明連結（可在 www.paypal.com 上獲取）。

相互協助

各方同意在合理必要的範圍內相互合作，以便另一方充分履行其在資料保障法下作為獨立控制方的責任。各方同意，如果商家收到主體存取要求，或收到客戶行使其在資料保障法範圍內任何權利的要求，商家應直接回覆此等客戶存取要求。商家應同時告知客戶，客戶可根據 www.paypal.com 的《私隱權聲明》所述指示，行使其與 PayPal 付款服務相關的資料主體權利。此外，如果在涉及任何安全事件的情況下，PayPal 自行決定其必須通知受影響的客戶，而 PayPal 沒有與受影響客戶通訊所需的聯絡方式，則商家僅得出於協助 PayPal 履行資料保障法規定的適用通知責任之目的，採用商業上合理的方式向 PayPal 提供商家可能擁有的客戶資料，以便 PayPal 通知受影響客戶。

跨境資料傳送

各方同意，PayPal 可以將根據本同意書處理的客戶資料傳送至收集該等資料的國家 / 地區之外，以便提供付款服務。如果 PayPal 將受本增編保護的客戶資料傳送至另一司法管轄區，而資料收集國家或地區的適用監管機構未對此司法管轄區作出適足性認定，則 PayPal 將確保根據適用的資料保障法，為傳送客戶資料採取適當

的安全保障措施。舉例來說，為符合 GDPR 的規定，我們會依據具有權限的監管機構核准的《PayPal 公司約束規則》及其他資料傳送機制，將客戶資料傳送至 PayPal 集團的其他成員。

對於你將其位於歐盟、瑞士、歐洲經濟區及 / 或其成員國或英國的客戶資料傳送至 PayPal 一事，各方同意：(i) 在適用範圍內，你簽署同意書一舉視為你這位商家作為資料匯出方和控制方，簽訂並接受歐洲委員會 2021 年 6 月 4 日關於根據 GDPR 向第三國家或地區傳送個人資料的標準合約條款之實施決定（歐盟法規編號：2021/914，下稱「歐盟傳送條款」），並視為其作為資料匯出方，簽訂並接受內閣大臣根據《2018 年資料保護法》第 17C(b) 條制定且目前在英國生效的法規中所規定的標準資料保護條款（下稱「英國傳送條款」）；(ii) 在適用範圍內，PayPal 簽署同意書一舉視為其作為資料匯入方和控制方，簽訂並接受歐盟傳送條款，並視為其作為資料匯入方，簽訂並接受英國傳送條款；並且，(iii) 各方應受歐盟傳送條款單元 1 的規定約束。若歐洲委員會或英國內閣大臣（或其他適用的英國主管機構）分別修訂並在此後公佈新的歐盟傳送條款或英國傳送條款（或歐洲委員會或英國內閣大臣（或其他適用的英國主管機構）另有要求或由其實行的情況下），各方同意，此類新的歐盟傳送條款或英國傳送條款（如適用）將會取代目前的歐盟傳送條款或英國傳送條款（如適用），並且各方同意採取所有必要的行動，以便執行新的歐盟傳送條款或英國傳送條款（如適用）。歐盟傳送條款（單元 1）和英國傳送條款將以提述方式納入同意書，並在本同意書生效後由各方嚴格執行，同時遵守以下詳細條款：

A) 歐盟傳送條款

1. 第 17 條（規管法律）之選項 1 應適用，並應由盧森堡法律規管此等歐盟傳送條款；
2. 根據第 18 條（訴訟場地選擇和司法管轄權），盧森堡法院將解決因此等歐盟傳送條款而產生的任何爭議；以及
3. 各方同意歐盟傳送條款附錄中所要求的詳細資料如附件 1 所述。

B) 英國傳送條款

1. 納入第 II(h)(iii) 條，並且 PayPal 簽署同意書一舉視為其作為資料匯入方為此條款提供必需的簡簽；
2. 各方同意英國傳送條款附錄 B 中所要求的詳細資料如附件 1 所述（在適用範圍內）。

附件 1

歐盟傳送條款附錄和英國傳送條款附錄 B

A. 以下內容根據歐盟傳送條款和英國傳送條款的規定適用

附錄 1.A. 締約方清單

資料匯出方

- 名稱及地址：資料匯出方為商家，地址如本同意書所述
- 聯絡人之姓名、職位和聯絡方式：如本同意書所述
- 與根據《標準合約條款》傳送的資料相關之活動：如本同意書所述
- 簽名和日期：請參閱本增編的「跨境資料傳送」部分
- 角色（控制方 / 處理方）：控制方

資料匯入方

- 名稱及地址：資料匯入方為根據本同意書提供服務之 PayPal 集團成員，其地址如本同意書所述
- 聯絡人之姓名、職位和聯絡方式：如本同意書所述
- 與根據《標準合約條款》傳送的資料相關之活動：如本同意書所述；簽名和日期：請參閱本增編的「跨境資料傳送」部分
- 角色（控制方 / 處理方）：控制方

附錄 1.B. 傳送說明

資料主體

傳送的個人資料涉及以下資料主體：

- 資料匯出方及其客戶、員工或其他商業往來方。

傳送的個人資料類別

傳送的個人資料可能包含以下資料類別：

- 姓名、支付金額、日期 / 時間、銀行戶口詳細資料、付款卡詳細資料、CVC 代碼、郵政編碼、國家或地區代碼、地址、電郵地址、傳真、電話、網站、到期資料、運送資料、納稅身份、客戶唯一識別碼、IP 位址、位置及 PayPal 根據本同意書收到的任何其他資料。

敏感資料（如適用）及採用的限制或保障措施

傳送的個人資料涉及以下敏感資料類別：

- 不適用，除非商家設置服務以取得此類資料。

採用的限制和保障措施：

- 不適用，除非商家設置服務以取得此類資料。

處理的性質

- 如本同意書所述。

傳送目的

資料傳送出於以下目的：

- 資料匯入方根據本同意書向資料匯出方提供的服務表現。
- 確定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欺詐性活動及其風險。
- 遵守適用於資料匯入方的法律。
- 如本資料保障增編所述的目的。

個人資料的保留期限；或無保留期限時用於確定此期限的標準

資料匯入方僅在實現收集個人資料之相關目的（請參見上述目的）所需的時間內保留個人資料。為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；未經授權使用或披露個人資料可能造成的損害風險；處理個人資料的目的以及這些目的能否透過其他方式實現；以及適用的法律、法規、稅務、會計或其他要求。

向（子）處理方傳送資料時，亦須註明處理的內容、性質及時間

資料匯入方可能會向第三方服務供應商分享個人資料，這些第三方服務供應商根據資料匯入方的指示及代表其執行服務和功能。舉例來說，這些第三方服務供應商可能根據本同意書提供服務元素（例如客戶認證、交易處理或客戶支援），或向資料匯入方提供服務以支援根據本同意書提供服務（例如儲存服務）。在確定第三方服務供應商進行資料處理的時間時，資料匯入方應採用本附錄 1.B. 中的上述標準。

附錄 1.C. 監管機構

根據歐盟傳送條款第 13(a) 條，負責確保資料匯出方在資料傳送方面遵守歐盟 2016/679 號法規的監管機構，應如條文所示作為主管監管機構行事。

附錄 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. 假名化、加密與傳送期間的資料保障。

PayPal 政策會確保遵守此原則，並要求使用技術控制措施以防止個人資料洩露的風險。PayPal 會對所有傳輸中及靜態個人資料採用加密技術。我們亦會採用業界標準的假名化技術，例如在適用情況下採用標記化方式來保護個人資料。PayPal 設有全面的政策，當中列出關鍵的義務和程序，以便保護在企業在內部以及向外部第三方傳送的資料。

2. 變更管理和業務延續性。

PayPal 設有強大的變更管理程序，透過確保變更均經過恰當的計劃、核准、執行和審查，在整個資料和系統生命週期內保障資料和系統持續可用和可彈性恢復。公司的業務延續性管理程序提供建立組織彈性恢復的框架，並讓公司能夠作出有效回應，以便保障其關鍵持份者的利益。

3. 災難復原。

PayPal 強大的災難復原計劃包含多項程序，可在發生任何重大中斷情況下復原資訊或技術系統，當中以支援重要業務程序和客戶活動的 IT 系統為主。PayPal 的技術基礎設施位於多個安全資料中心，這些中心分別具有主要和次要功能，並且均配備網絡與安全基礎設施、專用應用程式和資料庫伺服器及儲存裝置。

4. 定期測試、評定和評估技術及組織措施的有效性。

PayPal 定期規劃、執行和報告公司的測試計劃結果，以評定和評估其技術及組織措施的有效性。該計劃由我們的企業風險與合規團隊管理，他們與相關持份者合作，以便獲取並評估測試、報告及必要之補救所需的資料。

5. 用戶身份識別和授權。

PayPal 的存取權限管理程序要求用戶在存取任何其他適用範圍內的應用程式前，使用不重複的企業網絡帳戶 ID 和密碼登入企業網絡，以便進行用戶身份識別和驗證。當中採用有關密碼組成、長度、變更、重複使用和鎖定的自動政策。在所有適用範圍的系統中均實施基於角色的存取和核准措施（每季認證一次），以實行最低授權原則。

6. 個人資料處理地點之實體安全。

PayPal 全球安全和保安政策及程序根據適用的法律、法規和合作夥伴的要求，就促進可靠的安全和保安程序（包括實體安全）設定必要的要求。在根據公司的資訊安全處理標準建造郵件室、設備儲存區、運送和接收區域、電腦 / 伺服器室、通訊保存庫或機密文件 / 資料儲存區域等特殊或敏感區域時，我們特別著重安全系統和保障措施。

7. 事件記錄和配置。

PayPal 已概述並定義事件記錄和監察的類型及屬性。公司會收集並綜合多種類型的記錄至集中式安全監察系統。標準的配置管理控制措施經已設立，以便確保從系統中收集記錄，然後轉送到我們的集中式安全監察系統。PayPal 的政策與支援程序規定必須在所有系統中實施系統配置和加強基準。

8. IT 治理與管理；程序和產品的認證及保證。

PayPal 在公司上下推行強力的安全理念。我們的資訊安全總監負責監督全球企業內的資訊安全。作為「企業風險及合規管理」計劃的一部分，我們的「技術監督及資訊安全」計劃旨在支援公司管理技術和資訊安全風險，以及識別、保障、偵測及回應資訊安全風險並從中復原。PayPal 透過以下各種企業計劃來認證和保證其程序和產品，包括 (i) 對 PayPal 的技術行業標準義務進行審計和評估，包括但不限於 ISO 27001、付款卡行業 (PCI) 適用的標準 (DSS、PIN、P2PE 等) 和美國註冊會計師協會 (AICPA) SOC-1 及 SOC-2; (ii) 風險控制識別程序 (RCIP)，以便確保早期參與並採用標準方法來衡量、管理和監察與產品解決方案開發和發佈相關的風險; (iii) 在產品和軟件開發過程的早期階段納入私隱權影響評估; 以及 (iv) 全面的第三方管理計劃，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。

9. 收集最低限度的個人資料。

我們的政策規定並透過技術控制，收集和產生的資料應適當、相關，且僅限於與處理目的相關的必要範圍。由 PayPal 的私隱權影響評估程序確保遵守這些政策。

10. 資料品質與保留。

PayPal 的資料存取及品質政策確保所有個人資料正確、完整且為最新，可以讓個人用戶可存取系統以更正和修改其詳細資料（例如地址、聯絡方式等），並且可以在收到資料主體的更正要求時提供服務，以實現他們的更正權。我們的資料治理計劃會監察資料品質、問題和必要時的補救措施。我們規定所有資料均須根據 PayPal 的法律、監管和商業記錄保留要求，按其商業價值分類並指定保留期限。在保留期限到期後，資料和資訊均會處置、刪除或銷毀。

11. 問責制。

PayPal 已制定一套符合行業標準的資訊安全、技術、資料治理、第三方管理、私隱權之政策和原則，旨在讓持份者參與協作與合作，從而認識並在組織內部全面遵守此類政策和控制措施，以確保整個組織從上到下均參與其中並負責。每個計劃均闡明了與資料相關的跨職能決策、程序和控制措施的責任。作為資料控制方，PayPal 負責並證明其遵守 GDPR 及其他適用的資料保障法中涉及責任義務的相關

條款，方法為實施私隱權計劃政策和基本分層組織與技術控制結構，以確保整個企業遵守私隱權法律、法規、政策和程序。這包括能夠透過以下方式證明其遵守資料保障法：1) 建立強大的合規文化；2) 設立包括管理委員會、監督角色和私隱權報告的企業風險與合規治理結構；3) 確保業務職能負責任遵守私隱權計劃，包括建立、記錄和維持業務程序和控制；4) 由企業合規組織內的全球私隱權部門負責監督企業是否遵守私隱權計劃，並闡明由不同業務職能操作的政策、標準、程序和工具；5) 由全球私隱權職能向企業發佈通訊，以便促進對私隱權的認識和理解；6) 建立企業風險與合規管理框架，以便確保使用一致的程序，包括私隱權影響評估、私隱權監察與測試、私隱權問題管理、私隱權培訓和年度私隱權計劃；以及7) 向負責監督私隱權計劃的管理委員會提供報告和分析。

12. 資料主體權利。

PayPal 已制定一項計劃，以確保實現資料主體權利（包括存取權、更正權和刪除權）。除非 PayPal 有由法律法規賦予的義務或其他合法的商業理由可保留資料，否則將履行資料刪除要求。PayPal 的政策會確保在整個客戶生命週期內刪除資料。

13. 處理方。

PayPal 擁有全面的第三方管理計劃，可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。我們設有合約控制措施，要求我們的處理方及其子處理方在整個處理鏈中實行全面的資料安全和私隱權標準。所有子處理方在參與處理前都必須經我們事先核准。

B. 以下內容僅適用於英國傳送條款

接收方

傳送的個人資料僅可向以下接收方披露：

- 資料匯入方的服務供應商、分支機構和根據本同意書提供服務的人員。

匯出方的資料保障登記資料（如適用）

不適用。

其他有用資料（儲存限額及其他相關資料）

如本同意書及本附件 1 以上內容所述。