



全球隱私權政策

目錄

簡介	2
政策概觀	
範圍	
當地法律應用	
定義	3
資料保護原則	4
安全與存取	5
特殊情況	6
第三方資料傳輸或處理	
處理特殊類別個人資料	
電信與網際網路	
通訊與責任	7
相關政策	
反報復政策	
政策管理人	
通過日期	



簡介

政策概觀

FedEx Corporation (連同其子公司和附屬公司統稱「FedEx」) 瞭解設置有效隱私權保護措施的重要性，並致力於遵循適用的資料隱私權法律、規範、內部政策和標準。上述保護措施構成值得信賴的企業的基礎，也是維持客戶及員工信心所必要的，並可確保本公司遵循相關當地法律。本「全球隱私權政策」(簡稱「政策」) 乃根據全球通用的基本資料保護原則而建立。

範圍

本政策適用於 FedEx 全球所有員工與公司。獨立營運公司不得採納有悖於本政策的其他政策。獨立營運公司、區域或國家/地區適用的補充資料保護要求，必須經過全球法規遵循及監管首席官(「GCCGO」) 核准，始得建立。

當地法律適用

各 FedEx 營運公司有責任遵循本政策。若營運公司認為當地法規要求或其他法律義務與本政策規定之責任互相違背，相關公司必須通知 GCCGO。若適用的當地法律、規定或規範與本政策之間出現衝突，FedEx 將致力尋找可行解決方案，以調和上述這些要求。



定義

個人資料 — 可直接或間接用以識別自然人身份的任何資訊，不論該人是員工、客戶或客戶員工、廠商或廠商員工、求職者或任何第三方的身份。

範例：

- 姓名
- 政府核發的身分識別號碼 (社會安全碼、駕照號碼等)
- 地址
- 電話號碼
- 電子郵件地址
- 照片

處理 — 對個人資料執行之任何作業 (不論是否使用自動化系統)，例如：收集、儲存、統整、保存、封存、記錄、檢視、修正、改編、修改、提問、使用、擷取、轉寄、傳輸或結合資料。亦包含清除、刪除、消除、銷毀或封鎖資料。

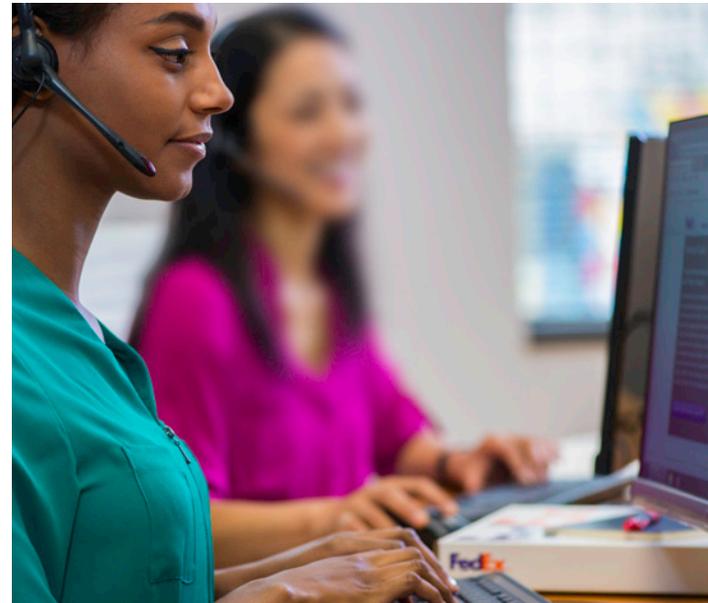
範例：

- 將資訊儲存在資料庫內
- 檢視儲存在其他電腦上的資訊
- 從資料庫傳輸資訊至另一資料庫

備註：

經匿名處理的資料 (無法識別該人) 即不構成個人資料。

運輸內含個人資料的物理媒體 (文件、電腦等) 並不構成個人資料處理作業。



資料保護原則

個人資料必須以正當且專業的方式收集、記錄及使用，不論該資料是以紙本、電腦記錄或任何其他方式記錄。

FedEx 負有責任且必須有能力遵循下列資料保護原則。

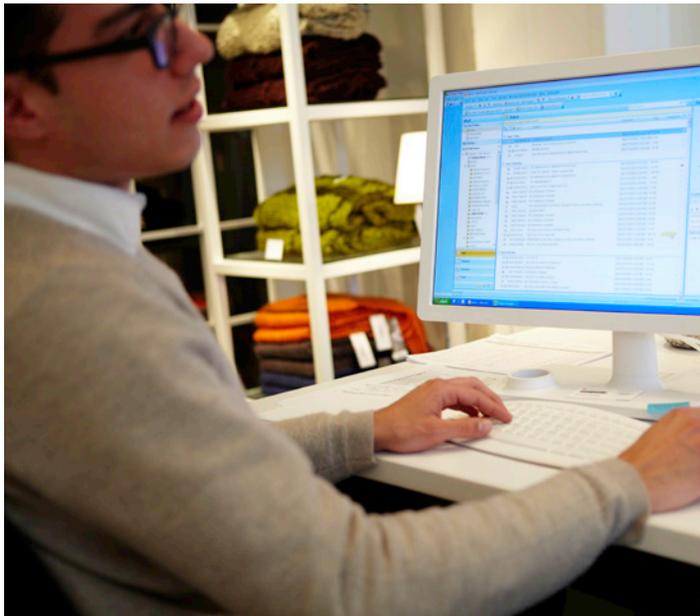
1. **公平合法**。處理個人資料時，個資當事人的權益必須受到保護。收集並處理個人資料時必須公平合法。
2. **用途詳述**。個人資料的使用或處理僅限用於收集時所定的用途，且不得以有悖於該用途之任何方式進一步使用或處理。不得以潛在的未來用途為理由收集和儲存個人資料，除非當地法律許可。
3. **收集限制**。FedEx 收集的個人資料僅限收集時所定用途所需內容，且不得超過當地法律許可限度。
4. **資料刪除**。個人資料若不再適用於收集時所需用途，應根據適用保存時間表予以刪除，除非屬於法務部門核准之例外情況。
5. **資料品質**。個人資料內容須準確，並在必要時及時更新。
6. **安全防護**。必須使用技術、管理和物理安全措施，保護個人資料，避免遺失風險或遭到未經授權的存取、破壞、使用、修正或洩露。
7. **資料透明度**。收集個人資料時，必須告知個資當事人其個人資料會被如何使用或處理。個資當事人必須清楚知曉資料收集者是誰、個人資料的處理用途，以及若有第三方經手處理其資料，則告知已設置充分的保護措施。所有此類告知必須先通過法務部門核准。
8. **個人參與**。在當地法律要求範圍內，個資當事人應有權存取其個人資料，並在適當情況下予以修正或刪除，以及行使當地法律提供的任何其他權利。



安全與存取

個人資料屬於機密資訊類別。嚴禁員工未經授權而處理此類資料。員工不得處理其合法職責範疇以外的資料。員工僅可存取所執行任務的類型和範圍所對應的相應個人資料。為此，必須定義、劃分並落實職務與責任。

嚴禁員工在 FedEx 職責範疇外使用個人資料、向未經授權人士洩露相關資訊，或以任何方式在業務許可使用範圍外提供此類資訊。主管人員必須在員工入職時，告知其應負保護個人資料之義務。即使員工離職，仍應繼續履行此義務。



必須保護個人資料，防範他人未經授權存取、非法處理或洩露個人資料。不論以電子或紙本形式處理資料，這個要求均適用。在引進新的資料處理方式前，應對新 IT 系統執行隱私權影響評估，評估的結果可能要求採取技術與組織層面的相關措施來保護個人資料。

員工必須遵循「FedEx 資訊安全標準」，搜尋關鍵字「標準」即可找到這個標準。「資訊安全」將所有資料分類成敏感、內部或公開資訊。您必須依資訊安全部的分類，遵循適用的「資訊安全標準」來保護個資。

若遇可疑活動、疑似網路攻擊、疑似安全事件或可能的個資違規行為，所有 FedEx 員工必須立即透過事件通知網站、搜索關鍵字「事件」或撥打 901/224-2021 或 901/224-2022 將上述事件向資訊安全部回報。

特殊情況

第三方傳輸或處理資料

您不得將個人資料傳輸至資料來源國以外的國家/地區，除非獲得法務部門核准，法務部門將確認已採取適當資料保護措施或合宜防護，方可傳輸。若廠商或第三方涉及處理個人資料，則必須與該外部供應商簽訂資料傳輸協議。外部供應商必須遵照 FedEx 相關指示進行個人資料處理。

處理特殊類別個人資料

您僅能在特定情況下，處理內容極度敏感之特殊類別個人資料。上述類別包含個資當事人的種族與民族、政治理念、宗教或哲學理念、工會成員身分，或健康狀況和性生活。依當地法律規定，可能有進一步細分的資料類別須特殊對待。與犯罪有關的個人資料通常可遵循當地法律的特殊要求進行處理。含有特殊類別資料的休假申請，須交由當地人力資源與法務部門處理。

若規劃實施含有特殊類別個人資料的新系統、相關程序或處理流程，則必須事前通知全球法規遵循及監管首席官 (GCCGO)。

電信與網際網路

所提供的電話設備、電子郵件地址、內部網站和網際網路，以及內部社交網路，主要用於所指派的工作。上述通訊方式可在遵循適用法規與內部政策的情況下使用。在少數可接受的私人用途情況下，必須遵守有關電信保密的當地法律以及任何當地電信法律。

通訊與責任

所有員工皆須負責：

- 閱讀並遵循此政策與相關政策規定，以及為實施本政策相關規定而制定並維持的相關文件/準則。
- 回報違反本政策的行為。

管理階層須額外負責：

- 確認所有下屬人員瞭解本政策規定。
- 確認已實施適當防護措施以保護個人資料。
- 提供所有必要訓練和/或指導，以協助實施本政策，並監控本政策的遵循情況。

相關政策

- [商業行為規範與倫理道德](#)
- [資訊安全標準](#)
- 所在公司的電腦資源使用政策
- 所在公司的職前審查政策
- 所在公司的招募政策
- 所在公司的資料保存與銷毀時間表
- 關鍵字「事件」

反報復政策

FedEx 嚴禁對善意舉報違反本政策可疑行為的人進行任何形式的報復。

政策管理人

全球法規遵循及監管首席官

通過日期

本政策已於 2018 年 5 月 1 日通過並生效。

