Dropbox

隱私權及資料保護

簡介

個人資料在社會和經濟中扮演著重要的角色。針對互動組織使用及保護個人資料的保護方式，人們日益要求握有更多控制權以及獲得清楚說明。

Dropbox 與全球數百萬使用者和公司間的關係都是建立於信賴上。我們非常重視您對我們的信任，並竭力保護您的個人資料安全。

我們對您的承諾

我們承諾保護您的個人資料。Dropbox 的《服務條款》列明您使用服務時，我們所負擔的責任。我們的《隱私權政策》則說明我們對使用者隱私權的承諾，並解釋在您使用服務時，我們如何收集、使用與處理您的個人資料。如果您居住在北美洲 (美國、加拿大與墨西哥)，Dropbox, Inc. 即爲您的服務供應商。

針對其他使用者，則由 Dropbox International Unlimited Company 負責控管您的個人資料。

如果您是 Dropbox Business 或 Dropbox Education 使用者，則由您的組織負責控管任何提供給 Dropbox，且與您使用 Dropbox Business 或 Dropbox Education 相關的個人資料。控管資料者可決定處理個人資料的目的與方式。若您使用 Dropbox Business 或 Dropbox Education，Dropbox 則爲資料處理者，代表您的組織處理資料。而我們的《企業協議》包含與資料處理和國際資料傳輸相關的承諾。

我們的優良紀錄：法規遵循

遵循法規的服務才值得信賴。我們鼓勵也樂意提供獨立驗證，證明我們的安全性和隱私權實務符合最廣爲採用的標準與規範，例如 ISO 27001、ISO 27017、ISO27018、HIPPA/HITECH、德國 BSI C5 與 SOC 1、2 與 3。

此外，我們也是第一批達到 ISO 27018 認證的雲端供應商，該標準經國際認可，是雲端隱私與資料保護作法的領先標準。我們的獨立第三方稽核員會測試我們的管控措施，並提供報告及意見。在可行的情況下，我們會與您分享這些資訊。

請注意，儘管這些認證和稽核報告通常針對 Dropbox Business 與 Dropbox Education 的服務範圍，但我們大多數的控制措施皆適用於 Dropbox Basic、Plus 與 Professional 使用者。如需進一步瞭解我們遵循哪些標準，以及驗證作法的方式，請參閱法規遵循網頁。

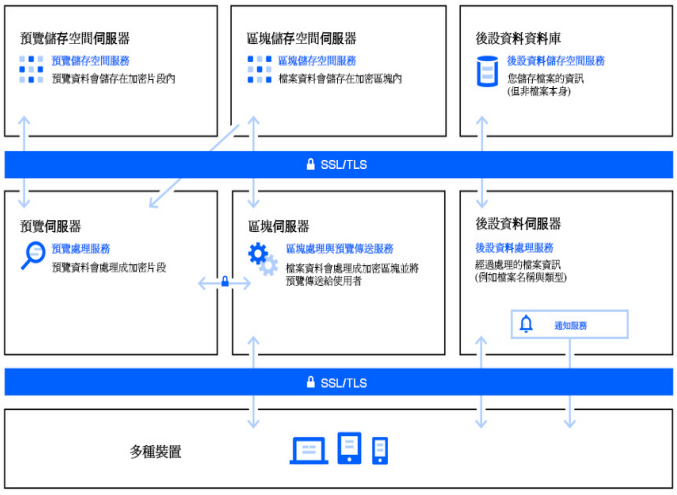
Dropbox

Dropbox 架構：保護您的個人資料

Drobpox 相信保護個人資料始於確保資料安全。爲達到此目標，Dropbox 擁有多層防護，提供安全的檔案資料傳輸、加密，並在具可擴充及安全的架構上提供應用程式層級的控制功能。

我們的系統架構：檔案

Dropbox 的檔案系統架構元件如下圖所示。



後設資料伺服器

使用者資料的特定基本資訊，又稱爲後設資料，會保存在其本身的儲存空間服務中，並作爲使用者帳戶的資料索引。後設資料包含基本帳戶與使用者資訊，例如電子郵件地址、姓名與裝置名稱。後設資料也包含關於檔案的基本資訊，包含檔案名稱與類型，可協助支援版本紀錄、復原與同步等功能。

後設資料資料庫

檔案後設資料儲存於採用 MySQL 的資料庫服務，且會視需要分區及複製，以協助系統達到效能與高可用性要求。

區塊伺服器

在設計上，Dropbox 提供超越傳統加密的安全機制以保障使用者資料。區塊伺服器處理來自 Dropbox 應用程式的檔案時，會把每個檔案切割成多個區塊，再用強大的編碼器將每個檔案區塊加密，只有不同修訂版本之間有經修改的區塊才會同步。Dropbox 應用程式偵測到新檔案或是現有檔案的變更後，會通知區塊伺服器，而新增或修改後的檔案區塊就會經過處理並傳遞至儲存空間伺服器。

區塊儲存空間伺服器

使用者檔案的實際內容會儲存在區塊儲存空間伺服器內的加密區塊中。在傳輸前，Dropbox 用戶端會將檔案分割成檔案區塊，爲儲存做好準備。區塊儲存空間伺服器爲可處理內容的儲存空間 (CAS) 系統，可依據雜湊值存取各加密檔案區塊。

預覽伺服器

預覽伺服器可用於產生檔案預覽。預覽爲以不同的檔案格式呈現使用者檔案，以便透過更合適且快速的方式在使用者裝置上顯示檔案。預覽伺服器會從區塊儲存空間伺服器上擷取檔案區塊，以產生預覽。提出檔案預覽要求時，預覽伺服器會從預覽儲存空間伺服器上擷取快取預覽，並傳遞至區塊伺服器。預覽最終會透過區塊伺服器呈現給使用者。

預覽儲存空間伺服器

快取預覽會以加密格式儲存於預覽儲存空間伺服器。

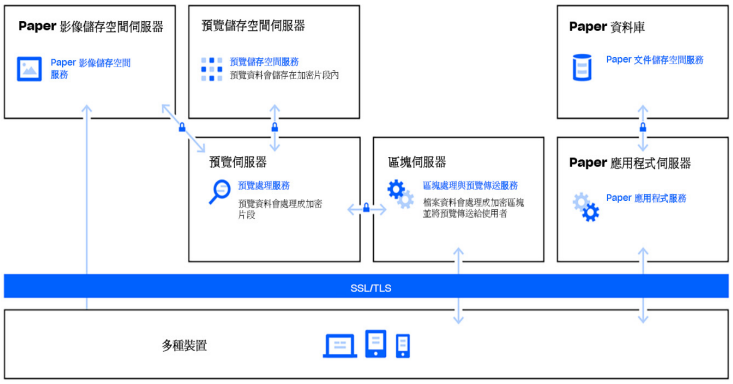
通知服務

無論是否在 Dropbox 帳戶中做出變更，個別服務都會受到監控。不會於此處儲存或傳遞任何檔案或後設資料。各用戶端會與通知服務建立長輪詢連線並等待。只要在 Dropbox 中變更任何檔案，通知服務就會關閉長輪詢連線，通知相關的用戶端有變更發生。關閉連線表示用戶端必須連接至後設資料伺服器，才能安全地同步變更。

Dropbox

我們的系統架構：Paper

Dropbox Paper (又稱 Paper) 是 Dropbox 產品的一項功能。然而，Paper 使用的是 Dropbox 系統架構環境內幾乎完全獨立出來的一組系統。Paper 的系統架構元件如下圖所示。



Paper 應用程式伺服器

Paper 應用程式伺服器負責處理使用者要求、把經編輯的 Paper 文件之輸出轉譯給使用者，以及執行通知服務。Paper 應用程式伺服器會將使用者的編輯寫入 Paper 資料庫，將這些資料存放至永續性儲存空間。Paper 應用程式伺服器和 Paper 資料庫的通訊工作階段，會以強大的編碼器加密。

Paper 資料庫

使用者 Paper 文件的實際內容，以及這些 Paper 文件的特定後設資料，都會以加密的形式存放在 Paper 資料庫的永續性儲存空間中。這包括 Paper 文件相關資訊 (像是名稱、共享成員和使用權限、專案和資料夾關聯等等多項資訊) 以及 Paper 文件本身的內容 (包括留言與工作項目)。Paper 資料庫會依需要分區及複製，以協助系統達到效能和高可用性的要求。

Paper 圖片儲存空間伺服器

上傳到 Paper 文件的圖片，會以待用的形式加密儲存於 Paper 圖片伺服器。Paper 應用程式和 Paper 圖片伺服器之間的圖片資料傳輸，會以加密的工作階段進行。

預覽伺服器

預覽伺服器會爲上傳到 Paper 文件的圖片，以及 Paper 文件內嵌的超連結提供圖片預覽。就上傳到 Paper 文件的圖片來說，預覽伺服器會透過加密管道，擷取儲存在 Paper 圖片儲存空間伺服器的圖片資料。就內嵌在 Paper 文件中的超連結來說，預覽伺服器則會使用取決於來源連結的加密方式，擷取圖片資料並轉譯成預覽圖片。預覽最終會透過區塊伺服器呈現給使用者。

預覽儲存空間伺服器

Paper 會使用 Dropbox 系統架構圖表中提及的預覽儲存空間伺服器，來儲存快取圖片預覽。快取預覽片段會以加密格式儲存在預覽儲存空間伺服器中。

Dropbox

Dropbox 管控功能：我們的內部實務

我們採取全面性的措施來保護系統架構、網路與應用程式。我們所採取的部分安全措施包含在儲存、傳輸與永久刪除檔案時進行加密處理。
我們也爲所有員工提供紮實的隱私權與安全性訓練，營造將信任視爲第一優先的文化。我們管控功能的部分詳細資訊如下所述：

訓練

保護使用者個人資料所需採取的措施，有一部分在於打造與培養具備安全性與隱私權意識的文化。Dropbox 員工必須先同意安全政策，包含使用者資料隱私權政策，才能獲得系統存取權。只有具備特定需求的員工才能存取上述系統。我們也強制員工參與年度安全性與隱私權訓練。

傳輸時加密處理

爲了保護在 Dropbox 用戶端 (目前爲桌面與行動應用程式、應用程式設計介面 (API) 或網頁) 以及 Dropbox 前端伺服器之間的檔案資料傳輸，我們已協調使用加密連線以保障資料安全傳送。同樣地，我們也協調使用加密連線保護 Paper 文件資料在 Paper 用戶端 (目前爲行動應用程式、應用程式設計介面 (API) 或網頁) 以及託管服務之間的傳輸。這些連線使用安全通訊端層 (Secure Sockets Layer，SSL)/傳輸層安全性 (Transport Layer Security，TLS) 加密，建立受 `128 位元或更高進階加密標準 (AES) 加密的安全通道。

儲存時加密處理

使用者上傳的檔案會以獨立檔案區塊的形式儲存於 Dropbox 的儲存空間伺服器。各區塊皆使用 256 位元進階加密標準 (AES) 加密。僅同步不同修訂版本間有修改內容的區塊。同樣地，儲存於 Paper 資料庫的 Paper 文件資料也在儲存時使用 256 位元進階加密標準 (AES) 加密。

永久刪除檔案與 Paper 文件

當 Dropbox 使用者以及 Dropbox Business 或 Dropbox Education 工作團隊的管理員標記永久刪除某檔案，就會觸發永久刪除該檔案的流程。同樣地，當使用者以及 Dropbox Business 或 Dropbox Education 工作團隊的管理員標記永久刪除某 Paper 文件時，也會觸發類似流程，以永久刪除該 Paper 文件與圖片資料。

個人資料存取要求

如需存取儲存在 Dropbox 上的檔案與 Paper 文件外的個人資料，使用者可以登入網站並前往他們的帳戶頁面。帳戶頁面會顯示與帳戶相關聯的資訊，如姓名與電子郵件地址等。使用者也可以從安全性頁面與連接應用程式頁面檢視連線工作階段、電腦與行動裝置的 IP 位址，以及連接至帳戶的應用程式。

Dropbox 使用者也可以選擇要求存取或刪除其他 Dropbox 可能收集的個人資料。您可於 Dropbox 的支援中心頁面找到更多關於此流程的資訊。

Dropbox 的隱私權治理

隱私權計畫團隊負責執行 Dropbox 的隱私權計畫。此計畫落實我們的關鍵隱私權措施，且在我們的資料生命週期設計中也將隱私權視爲優先事項。Dropbox 隱私權計畫進一步獲得許多跨部門的法務子團隊支持。這些子團隊可針對執行與監管日常隱私權計畫工作所需，提供額外專業知識。

例如，DPO 團隊獨立於其他隱私權部門運作，並提供隱私權法規遵循與監管，直接支援資料保護官執行職責。資料保護官 (DPO) 爲歐盟當地代表，聯絡方式：privacy@dropbox.com。

Dropbox

政府資料要求準則

我們明白使用者願意將個人資料交給我們，就是因爲信任我們一定會保密。如同其他線上服務，Dropbox 偶爾也會收到政府的要求，希望我們提供使用者資訊。

下列原則說明我們如何處理政府資料要求。

保持透明度

我們認爲，政府應許可線上服務公布他們接獲的資料要求次數和種類，也應有權通知資料遭要求的使用者。這類的透明度讓使用者得以更清楚地瞭解政府過度擴張的案例和型態。

我們會持續公布關於這些要求的詳細資訊，並爭取能夠公布更多相關重要資訊的權利。

反對過分廣闊的資料要求：

政府資料要求應只嚴格限於要求特定人士和合法調查事件的相關資料。我們反對地毯式、過分廣闊的資料要求。

提供可信賴之服務

政府不應在線上服務中植入木馬程式，或破壞其架構來取得使用者資料。我們會致力保護我們的系統，並要求政府修改法規，明定這類行爲違法。

保護所有使用者

據使用者的國籍和居住地給予特定保護的法律已過時，不符合全球線上服務的精神。我們會持續爭取改革這類法規。

我們已於 Dropbox 網站上公布這些原則，以及我們的年度透明度報告：https://www.dropbox.com/transparency。

如需關於我們的管控功能與我們保護個人資料方式的詳細資訊，請參閱我們的《Dropbox Business 安全白皮書》。

Dropbox 的協力廠商

大多數與提供服務相關的活動皆由 Dropbox 管理，然而，有些受信任的第三方也會介入與服務相關的某些部份 (例如客戶支援與 IT 服務供應商)。這些第三方只會在遵循我們隱私權政策，並代表我們執行工作時存取您的資訊，且我們仍爲第三方依照我方指示處理您的資料之一切過程負責。

每個第三方都需要通過嚴格的稽核流程，包含安全審查和定期合約審查，以確保他們的能力符合我們對資料保護的承諾。

國際資料傳輸

Dropbox 仰賴多種合法機制，以完成從歐盟到美國的個人資料國際傳輸。我們通過「歐美隱私屏盾」和「瑞士與美國隱私屏盾」認證隱私屏盾計畫涵蓋個人資料的收集、使用與保留，以及從歐盟和瑞士傳輸個人資料到美國的相關事項。除了隱私屏盾，Dropbox 也針對服務隱私權提供高強度的合約保證，並落實歐盟模式的合約條款，來保障國際資料傳輸安全。

Dropbox

GDPR：一般資料保護規則

一般資料保護規則 (又稱 GDPR) 是歐洲聯盟 (EU) 的一項法規，旨在建立處理一套保護歐盟資料主體個人資料的法律架構。

GDPR 是自 1995 年歐盟資料保護指令公布以來，最重要的歐盟資料保護法規，且包含 Dropbox 在內，許多在歐洲經營業務的公司，皆投資大量心力在遵循 GDPR。

GDPR 協調了歐洲各地的資料保護法規，並確保資料保護法規跟上過去二十年來快速的科技變化。

GDPR 立基於歐盟過往的法律架構，包含歐盟資料保護指令，並要求處理個人資料的組織負擔新的義務與責任，也爲個人就其個人資料提供新的權利。

管理個人資料。在歐盟境內的組織，以及處理歐盟資料主體個人資料的組織，皆須遵循 GDPR 的規範。

Dropbox 的 GDPR 法規遵循之路

Dropbox 致力於遵循 GDPR 規定。我們從一開始就重視業務上的隱私權與安全性，隨著我們的成長，我們始終致力保護客戶信託於此的個人資料，並把這視爲第一要務。Dropbox 長期在規範遵循上保持領先紀錄。舉例來說，我們是第一批爲商業使用者達到 ISO 27018 認證的雲端服務供應商。這個強大的基礎讓 Dropbox 將 GDPR 法規遵循視爲現有實務與控管措施的補強，並象徵我們的措施不斷演進，以始終確保使用者資料受到保護。

Dropbox 的 GDPR 法規遵循之路，早在 2016 年法規公布時即啓程。當時，我們邁出的第一步是建立一個跨部門的資料保護專家團隊，陣容包含法律顧問、安全與法規遵循專家、產品與系統架構工程師等。我們的團隊徹底就 GDPR 的要求，針對我們現行的安全性與資料保護措施進行全面評估。

我們的下一步則是評估個人資料處理活動，並追蹤整個系統內的個人資料生命週期。這些做法有時被稱爲執行資料對應與完成資料保護影響評估。

Dropbox

支持使用者踏上他們的 GDPR 之路

Dropbox 提供控制與能見度功能，協助您更輕鬆地管理包含 GDPR 在內的資料保護法規遵循義務。當然，與 Dropbox 等供應商建立關係，絕非您整個組織開始遵循 GDPR 的起點或終點。儘管我們的功能可協助管理您的義務，並不能確保您確實遵循這些義務。遵循 GDPR 需要您更深刻地思考組織內的資料移動和保護方式。每個組織都應該用自己的方式來完成法規遵循，而供應商是這趟旅程中的重要夥伴。

資料最小化

GDPR 的隱私始於設計要求中，一項重要元素是要求組織應以資料最小化的方式設計其服務。這表示組織必須針對資料提供優良的能見度與管控功能，以便使用者管理資料。Dropbox Business 管理員資訊主頁是一項可協助您管理資料的實用工具，讓您得以監控工作團隊活動、檢視連接裝置並審核共享活動。我們致力於將隱私始於設計原則加入新產品和功能中。

資料的保護與還原

遺失裝置保護、版本紀錄與檔案復原可避免意外遺失、損壞或破壞個人資料，且在意外發生時，可即時協助還原個人資料的可用性與存取。雙因素驗證是另一項我們鼓勵您採用的資料保護措施。

保留紀錄

GDPR 日益要求組織負擔維持處理活動的詳細紀錄之義務。我們的稽核記錄檔與我們的活動紀錄能協助您進一步瞭解您的處理活動，並支援您保留紀錄。

存取權管理

您可於 Dropbox Business 管理員資訊主頁內輕鬆管理工作團隊成員對檔案、資料夾與 Paper 文件的存取權。針對共享檔案連結，我們的存取權限功能，讓您可以使用密碼保護共享連結、設定到期日以限定存取時限，並限制僅有組織內成員才擁有存取權。在使用者職責變更時，我們的帳戶移轉工具讓您得以輕鬆將 Paper 文件的檔案和所有權移轉給另一位使用者。

管理員也可以停用使用者對帳戶的存取權，但仍能保留他們資料與共享關係，以確保組織資訊安全。最後，遠端清除功能讓您得以從遺失或遭竊的裝置上清除檔案與 Paper 文件。

歐盟系統架構

儘管 GDPR 並未要求在歐盟境內託管個人資料，Dropbox 確實提供符合資格的 Dropbox Business 與 Dropbox Education 客戶在歐盟境內儲存檔案 (區塊) 的選項。在歐盟境內的檔案儲存空間由 Amazon 網路服務 (AWS) 系統架構提供。如需深入瞭解我們的歐盟系統架構，請聯絡我們的銷售團隊。

Dropbox

同心協力，攜手保護您的個人資料

Dropbox 會與使用者合作，一起保護個人資料。我們採取全面性的措施來保護系統架構、網路與應用程式，並訓練員工採行安全性與隱私權實務、營造將信任視爲第一優先的文化，以及讓我們的系統與實務接受嚴格的第三方測試與稽核。

然而，使用者在保護個人資料方面也扮演重要角色。Dropbox 讓您可透過符合組織隱私權、安全性和法規遵循需求的方式設定、使用和監控帳戶。我們的《共享責任指南》可幫助您深入瞭解我們如何確保您的帳戶安全，以及您可以採取哪些行動來維持個人資料的能見度和控制。

摘要

每天都有數百萬名使用者表示信賴，將他們的資料託付給 Dropbox。爲了值得他們的信任，Dropbox 已落實並持續發展對安全性與隱私權的重視。我們承諾，所有的決策都會考量如何保護使用者的個人資料。如需更多資訊，請傳送電子郵件至 privacy@dropbox.com。若要深入瞭解 GDPR，也可以造訪我們的 GDPR 指引中心。