

安全控管





01	前言
02	法規浪潮來襲
03	面臨壓力的產業
04	五步驟計畫
05	結語



O1

前言



現代企業的動力來自團隊的協同合作，跨團隊、區域和組織共用資料，不但能推動創新、提升團隊效率，還能加速業務成長。然而，這種開放性往往與資料安全和法規遵循的要求相衝突，為企業帶來複雜的難題。

一旦沒處理好，需要面臨的後果十分嚴重。光是 2024 年，歐盟境內違反《一般資料保護規則》(GDPR) 而遭判罰金的案件就多達 277 件，總額高達 11.9 億歐元¹。舉例來說，Meta 在未採取適當防護措施的狀況下，將歐盟使用者資料傳輸至美國，因而遭處 12 億歐元罰款²。這類重大案件凸顯了不遵守法規會導致的財務和聲譽損害。

企業面臨的挑戰核心在於資料主權，也就是使用者控管資料儲存位置、存取方式和處理權限的能力。隨著歐盟、美國和全球其他地區的法規不斷演變，維護資料主權變得越來越重要。企業必須保護資料，避免未經授權的存取，同時遵守日益複雜的區域法律。這對資訊長、資安長和法規遵循主管來說是一大難題，因為他們推動資料保護計畫時，往往會遇到內部阻力。

資料來源：1. <https://www.enforcementtracker.com/?insights> 2. https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

Google Workspace 的安全控管功能可將資料區隔到不同地區，並選擇在何處處理及儲存資料，例如歐盟或美國，有助組織遵守嚴格的法規。有了精細的管理控制項，就能確保資料受到保護，排除未經授權的存取，同時實現安全流暢的協作。

本指南提供實用藍圖，協助您保護資料，並正面迎戰法規遵循的難題。從評估現有環境到落實進階控制，您將獲得所需的洞察資訊和工具，輕鬆應對資料主權的複雜議題。



要在強調協作的環境中實現資料主權，組織必須：

01

控管資料的儲存和處理位置。

02

確保只有授權者能存取。



02

法規浪潮來襲



世界各國政府都推出更嚴格的資料保護法，保障個人資訊，確保在當地控管敏感資料。這些架構正在重塑企業管理資訊的方式，為法規遵循和創新提供了新契機，也提高不合法規的風險。





歐盟： GDPR 和《歐盟人工智慧法》

《一般資料保護規則》(GDPR) 確立了全球資料隱私權的基準，嚴格規範個人資料的儲存、處理和移轉方式，尤其是移轉至歐洲經濟區 (EEA) 以外的地區。為符合規定，組織必須實施適當的防護措施，例如標準合約條款或同等保護措施。無論企業總部設於何處，只要向歐盟公民提供商品或服務，或監控他們的行為，就必須遵守 GDPR。



《歐盟人工智慧法》(EU AI Act) 是全球首部 AI 法律架構，旨在規範風險，並在歐洲推動值得信賴的 AI 用途。無論公司總部設於何處，只要在歐盟市場開發或部署 AI，都必須遵守這項法規。AI 系統分為四個風險等級：

不能接受的風險

禁止以威脅人類安全和權利的方式使用 AI (例如：社會信用評分、生物辨識監控)。

高風險

AI 在醫療照護、執法等重要領域必須遵守嚴格法規，包括風險評估和人類監督。

資訊公開風險

聊天機器人、生成式 AI 等 AI 系統必須清楚揭露 AI 生成的內容。

風險極低或沒有風險

低風險 AI (例如垃圾郵件篩選器、AI 輔助遊戲) 不受到限制。



美國： HIPAA、CCPA 及 CDPA

雖然美國沒有統一的聯邦資料隱私權法律，但產業和州級法規仍規定了重要義務：

《健康保險流通與責任法》(HIPAA)

適用於醫療照護機構、保險公司及相關業務夥伴，透過嚴格的隱私權和安全措施，保護病患資訊。

《加州消費者隱私法》(CCPA)

賦予消費者個人資料相關權利，包括存取、刪除或選擇拒絕銷售個人資料。適用於符合特定收益或資料門檻的企業。

《維吉尼亞州消費者資料保護法》(CDPA)

這項法律與 CCPA 類似，同樣以消費者隱私為目標，但強調資料最小化和透明度。

亞太地區： APPI 及 PIPA

01

日本《個人資訊保護法》(APPI)：著重於跨境資料傳輸，處理日本公民的資料時，必須取得同意或採取同等保護措施。

02

韓國的《個人資訊保護法》(PIPA)：強制執行嚴格規定，包括限制跨境傳輸，以及對違規行為處以嚴厲處罰。

南美洲： 巴西 LGPD

巴西的《一般資料保護法》(Lei Geral de Proteção de Dados，簡稱 LGPD) 與 GDPR 類似，要求嚴格取得資料處理同意聲明，並對違規行為處以重罰。適用於處理巴西公民相關資料的企業。



跨境傳輸的複雜性

跨國移轉資料時，必須遵守多項法規架構。

不斷變化的規定

隨著 GDPR 和 LGPD 等法律持續演變，組織必須調整做法，才能確保符合規定。

產業間的細微差異

法規通常會重疊，但會根據產業特有的風險和需求，以不同方式適用。

各架構的常見挑戰

儘管各地情況不同，企業面臨的挑戰卻大同小異。

這些架構是資料主權的法律基礎，但對處理機密資料的產業影響最深。請繼續閱讀，瞭解金融、醫療照護和科技等產業如何因應這些獨特挑戰。



03

面臨壓力的 產業

資料主權挑戰對各產業的影響不盡相同，某些產業因處理使用者私密資料，且受到嚴格的法規限制，會面臨更嚴峻的挑戰。

對於金融、醫療照護、政府和科技等產業，資料主權不僅僅是為了遵守法規要求，更關乎保護重要資產、建立利害關係人的信任，以及確保在日益複雜的環境中保持營運順暢和安全。

 共用



金融業： 在競爭激烈的市場中維護信任

由於客戶資料的私密性，以及金融機構在全球經濟中扮演的角色，金融業一直受到嚴格審查。GDPR 等法規要求精確控管資料儲存和存取權，而開放銀行計畫則要求安全地與第三方供應商分享客戶資料，促進創新。



方雪麗

重要注意事項：

跨境挑戰

跨多個司法管轄區管理財務資料會產生風險，特別是當資料在監管要求不同的地區之間流動時。

系統陳舊

許多銀行仰賴過時的基礎架構，難以採取進階加密或角色型存取權等現代化法規遵循措施。

聲譽風險

在這種信任至上的產業，只要有一次的資料侵害事件或未遵循法規，都可能導致嚴重的財務和聲譽損失。

金融機構可透過精細的存取權控管和本地化資料處理等解決方案，在符合法規標準的同時，維護客戶信任。



醫療照護業： 兼顧隱私與進步

在醫療照護領域，保護病患隱私是法律義務，也是道德承諾。醫療照護產業必須在保護敏感醫療記錄，以及推動醫療研究合作之間，取得微妙平衡。

重要注意事項：

法規重疊

醫療照護機構必須同時遵守多項複雜的法規，例如美國的 HIPAA 和歐盟的 GDPR，這些法規對資料儲存、加密和存取都有各自的標準。

跨國合作

研究機構通常需要分享資料至境外，這會使法規遵循作業更加複雜。舉例來說，在進行全球臨床試驗時，分享匿名病患資料必須符合當地資料主權法規。

營運中斷

過時的系統和孤立的資料往往導致效率低落，更在法規遵循稽核期間增加風險。

完善的資料保護措施，例如端對端加密和即時監督工具等，能確保醫療照護機構符合法規，同時促進創新與協作。



政府機關： 維護民眾信任與國家安全

政府機構管理大量私密的公民資料，包括稅務記錄和國家安全資訊。這項責任重大，保護這些資料不僅是法規遵循要求，也關乎公眾信任和國家安全。



重要注意事項：

地緣政治風險

政府機構面臨獨特的挑戰，包括網路威脅和外國勢力的壓力，因此資料落地和主權至關重要。

資訊公開與安全保障

在開放性與嚴格資料控管之間取得平衡，是維持公眾信任的關鍵。

區域法律

政府機構必須同時遵守多項法規，例如歐洲的 GDPR 或要求資料在地化的當地法令。

有了端對端加密和嚴格的存取控管等資料主權工具，公部門機構就能確保資料安全，同時兼顧透明度和作業效率。



科技業： 在嚴格審查下不斷創新

科技公司必須兼顧拓展全球營運和遵循區域法規，跨國處理大量使用者資料。對這些組織而言，資料落地不僅是法規遵循問題，更是保護智慧財產和維持客戶信任的關鍵。

「如果不能實施資料分區，或是將資料交由其他技術供應商處理，不僅我國和全歐洲將面臨風險，Airbus 也將陷入險境，這樣的風險我們承擔不起。」

Airbus 的 Sebastien Aubineau

重要注意事項：

全球營運與在地規則

Airbus 等公司強調，區域化資料處理對於保護私密資訊和遵守主權法規至關重要。

可擴充的解決方案

科技公司必須導入相關系統，才能在不違反法規的情況下拓展全球業務。

新興風險

快速創新往往會導致無法預期的安全漏洞，例如第三方應用程式整合和存取權控管不足。

科技公司可透過精細的管理員控制項和進階安全措施，克服這些挑戰，同時兼顧創新與成長。



04

五步驟計畫



如要確保資料主權，必須根據自身需求、產業和所在地，量身訂作有條理的做法。本指南列出五個步驟，協助您控管資料環境、遵守法規，安心執行組織的法規遵循策略。

01

評估環境

瞭解資料的儲存位置、誰有存取權限，以及適用的法規，這是找出缺口的起點。

02

選擇資料地區

將資料儲存和處理作業在地化，符合法規要求，同時維持營運彈性。

03

調整存取權 控管機制

調整權限，確保只有適當人員能存取適當資料，將資料外洩風險降到最低。

04

強化資料保護

強化安全措施並保護私密資料，有效防範日新月異的網路威脅。

05

報告與監督

持續監控及製作報表，在不斷變動的監管環境中，確保符合法規並採取主動措施。



01

評估環境

每段旅程的起點，都是瞭解現狀和目標。

如要因應資料主權問題，首先要瞭解您所屬產業的外部法規，以及內部資料環境的實際情況。也就是說，您必須瞭解資料的儲存位置、存取方式，以及該如何做才能符合法規要求，同時找出目前做法的不足之處。



瞭解法規內容

GDPR、ISO 和 SOC 等全球架構為法規遵循奠定基礎，但這些法規並非獨立存在，組織應視自身的特定營運需求擬定做法：

GDPR (歐洲)

除非有標準契約條款等適當防護措施，否則必須嚴格遵守歐洲經濟區 (EEA) 的資料落地規定。對於有歐洲客戶的組織來說，瞭解個人資料的儲存和移轉地點至關重要。

《歐盟人工智慧法》 (歐盟)

《歐盟人工智慧法》為歐盟法規，旨在為歐盟內部的人工智慧技術建立共同規範架構，並將人工智慧系統與模型分門別類，針對各類別施行不同要求。自 2024 年 8 月 2 日起，該法案正式具備法律效力。

DORA (歐盟)

《數位營運韌性法》(DORA) 制定技術標準，強化金融機構的 IT 安全性。這項法規由歐洲監管機構 (ESA) 制定，並經歐盟執委會採納，統一了金融業和資通訊第三方供應商的營運韌性規則。

SOC 法規遵循 (美國)

服務組織控制報告著重於安全性、可用性和機密性等信賴原則。如要符合美國會計師協會 (AICPA) 制定的這些標準，必須進行嚴格的內部稽核，並確保營運透明度，這對美國境內的組織或與美國實體交易的組織來說尤其重要。

ISO 標準 (全球)

由國際標準化組織制定，提供全球公認的資安管理架構。這些標準對在歐盟、美國和亞太地區等區域營運的跨國組織至關重要，有助於制定一致的資安政策。



檢視資料

下一步是從公司內部著手，整理資料環境的現況。資料儲存在哪裡？哪些人擁有存取權？公司現有系統有哪些不足之處？回答這些問題是制定法規遵循策略的基礎。

例如：

- 醫療照護機構可能會發現，私密的病患資料儲存在多個雲端服務中，且加密等級不一。跨國研究資料共用作業，會讓遵循 GDPR (歐洲) 和 HIPAA (美國) 法規更加複雜。
- 在這種情況下，進行資料稽核時可能會發現風險，例如未加密的記錄或不明確的存取權限，必須解決這些問題才能符合法規要求。

將這些洞察資訊與外部法規相結合，組織就能縮小法規遵循要求與營運實務之間的差距。





組建團隊

資料主權不僅是技術挑戰，也是合作挑戰。打造適合的跨職能團隊至關重要：

- **IT 主管**可描繪出目前的技術基礎架構，並解決加密或儲存空間不足的問題。
- **法務團隊**可解讀地區法規要求，確保合約符合法規遵循需求。
- **業務單位**可協助找出對日常營運的實際影響，例如存取權限和工作流程中斷。

整個團隊應共同努力，根據各區域的 GDPR、SOC 或 ISO 等架構要求，調整內部程序。

主動規劃

隨著法規和業務需求不斷演變，組織應立即採取行動，擺脫被動因應法規的局面，建立可支援未來成長的架構。

舉例來說，採用 **Google Workspace 的安全控管**等解決方案可奠定基礎，滿足資料落地和存取權需求，在確保法規遵循的同時維持靈活性。





資料落地與存取權控管

02

資料落地不僅關乎資料的存放位置，還包括確保您能控管資料的儲存、存取和處理方式，同時兼顧效能、擴充性和法規遵循。

對於處理大量機密資料的組織，Google Workspace 的安全控管功能等工具可簡化法規遵循作業，同時確保業務運作不受影響。

「我們對區域內資料處理進行了詳盡分析，過程順暢無礙，不必再花費高昂成本整合複雜的第三方服務。而且，我們沒有遇到任何故障或延遲，一切運作順暢。」

Randstad 全球協作產品負責人
Roman Spantgar

本地資料落地與彈性

許多組織面臨的難題，在於如何兼顧嚴格的資料落地要求和營運靈活性。舉例來說，若想拓展全球業務，組織通常需要同時符合地區法規和達成成效。

這會產生一個常見的難題：組織如何遵守法規，同時避免建立阻礙協作的孤立系統？Google Workspace 安全控管功能提供精密的彈性調度，可解決這個問題。您能定義資料的儲存和處理位置，同時維持雲端擴充性。跨國企業可為個別團隊、部門或地區設定資料落地政策，同時確保協作效率不受影響。

資料處理：不只是儲存空間

許多組織非常重視資料儲存位置，卻忽略處理位置，而這正是 GDPR 等法規架構的關鍵遵循要素。資料處理是指如何使用、分析或分享資料，通常需要比單純儲存資料更嚴格的監管。安全控管功能不僅提供儲存空間，還可將儲存空間和處理作業本地化，確保組織全面符合主權要求。





確保未來營運不受法規變動影響

資料主權的定義不斷演變，政府持續修正現有的法規並推出新法，更為企業帶來不確定性。如果系統設計過於僵化，僅能符合現今的法規，未來可能難以因應變化。Google Workspace 的安全控管功能可讓您靈活調整資料落地政策，因應法規變動。無論是跨區域遷移資料，還是調整存取控管機制，目標都是確保主權態勢與時俱進。

美國醫療照護法規遵循指南

《健康保險流通與責任法案》(HIPAA) 等聯邦法律為病患資料保護制定了全國一致的標準，但州級法律則增加了複雜性。《加州消費者隱私法》(CCPA) 和《維吉尼亞州消費者資料保護法》(CDPA) 等法規，對資料隱私權、消費者權利和資料保留期限，訂定了更嚴格的要求。在地化資料處理服務，能讓醫療照護機構更有自信應對這些重疊的規定。





03

調整存取權控管機制

資料安全儲存後，下一步就是確保存取權也受到同等保護。組織可實施最小權限原則，確保只有真正需要的人才能存取機密資訊。透過嚴格控管資料存取權，組織就能降低意外洩漏、內部濫用及第三方安全漏洞的風險。



存取控管的重要性

在現今的環境中，資料存取權若不加以限制，將成為日益嚴重的風險。內部過度授權會增加資料外洩和錯誤，第三方存取權則可能使法規遵循作業變得複雜。此外，《一般資料保護規則》(GDPR)、《健康保險流通與責任法案》(HIPAA) 和其他法規架構都要求嚴格控管機密資訊的存取權。



如何調整存取權

有了合適的工具，組織就能實施更聰明、安全的存取政策：



零信任架構

「絕不信任，一律驗證」的原則可確保每位使用者、裝置和連線都經過驗證和授權，即使是內部使用者也不例外。

資料存取透明化控管機制與存取許可

落實明確要求第三方存取權的工作流程。Google Workspace 的存取權核准等工具，可確保支援團隊只在絕對必要時存取資料，並提供完整的資料存取權控管與監控功能。

角色式存取控管 (RBAC)

將權限與特定角色對應，可將不必要的風險降至最低。例如：

- 財務團隊可存取付款系統，但無法存取人資記錄。
- 醫療照護機構人員可查看病患照護資料，但無法存取行政檔案。
- 支援團隊必須獲得明確核准，才能在有限時間內存取資料。

用戶端加密

多一層安全防護，可確保企業管理自己的加密金鑰，防止雲端供應商存取機密資料。

只要實施精細的存取權控管機制，組織就能兼顧安全性和法規遵循，同時滿足現代化協作的需求。在下一個步驟中，我們將探討如何強化安全措施，進一步降低風險，確保組織能持續領先，應對不斷演變的網路威脅。



限制存取權不僅是為了安全，更是為了提升作業效率。

作業效率：

將資料儲存在靠近使用者的位置，可縮短延遲時間、提高工作效率，並確保團隊無論身在何處都能順暢工作。

法規遵循：

將資料保留在當地，可避免法律風險，並確保符合 GDPR、HIPAA 和其他不斷演進的法規等架構。

安全性和資料遺失防護 (DLP)

04

資料安全儲存且存取控管機制完善後，下一個重要步驟就是保護組織免受日新月異的威脅侵擾。Google Workspace 的安全控管功能提供進階用戶端加密、精細的存取權控管機制，以及強大的資料遺失防護 (DLP) 工具，確保資料在儲存、傳輸或使用階段都安全無虞。





防範威脅十分重要的原因

現今組織面臨的資安挑戰日益複雜：

- **外部威脅**：網路釣魚攻擊、惡意軟體和未經授權的存取行為日益複雜，組織需要主動採取措施，保護機密資訊不受不肖分子侵害。
- **內部風險**：過度授權、意外分享和人為錯誤，仍是資料侵害事件的主要原因。加強存取權控管並嵌入技術防護措施，能降低這些安全漏洞的影響。

員工每天使用的工具 (例如瀏覽器擴充功能、效率提升應用程式或第三方整合服務) 可能會帶來意想不到的安全漏洞。無論是未經審核的應用程式分享機密資料、過度授權，還是遭受惡意軟體攻擊，這些風險都會為您的安全防護機制增加一層隱形的複雜性。

那麼，如何在保護重要資料的同時，確保員工能順暢使用所需工具呢？

Google Workspace 的安全控管功能可讓機構兼顧彈性和安全性：

- **精細權限**：限制第三方工具的存取權，確保機密資料不會外洩，並減少不必要的曝光。
- **用戶端加密**：提供端對端資料防護，即使員工在不同雲端服務中協作，也能確保資料安全。加密可防止未經授權的應用程式或服務讀取機密資訊。
- **瀏覽權限與核准**：隨時掌握工具使用情況、及早找出潛在風險，並只在真正必要時核准外部存取權。

安全控管功能內建這些控管機制，讓組織能確保安全無虞，同時賦予員工自由創新的空間。如此一來，工具才能發揮作用，不會傷害組織。

增添多層防護

安全控管功能也與零信任架構完美整合，採用「絕不信任，一律驗證」的原則，在存取機密資料前，要求每位使用者、裝置和連線都必須證明自己具有憑證。

無論是分享檔案前先加密，還是要求第三方存取權時須經過多層核准，這些技術控管措施都能確保安全防護機制隨時主動運作。



資料遺失防護的重要性

資料遺失防護 (DLP) 政策在強化安全防護機制方面扮演重要角色，可讓您：

- **監控資料移動：**追蹤機密資料在系統中的流動情形，找出並解決外洩或未經授權的分享行為。
- **設定自訂政策：**定義規則，自動封鎖、警告或標記違反法規的資料共用行為。
- **保護敏感資料類別：**找出特定資料類型，例如個人識別資訊 (PII)、財務資料或智慧財產，並加以保護。



資安通常被視為協作的阻礙及額外要處理的痛點。但實際上，資安能協助企業安心營運。安全控管功能提供進階加密、主動式資料遺失防護政策和核准程序，讓組織在保護機密資料和促進協作之間取得適當平衡。

在下一節中，我們將探討如何透過報表和監督機制，在不斷變動的法規環境中保持主動，確實遵守法規。



報表與監督： 透過資訊可見度建立信任

05

維護資料主權的工作並非在控管機制到位後就結束，而是要進一步證明這些機制有效。透過報表和監督機制，組織可以監控、稽核及調整資料策略。持續掌握加密、存取權和儲存空間的相關資訊，確保符合法規要求。對 Randstad 這類公司來說，即時報表工具可簡化稽核作業，順利遵循法規。

「實施資料地區後，對我們在歐盟處理個人資料的策略有重大影響。整個過程非常順暢，我們沒有遇到任何營運問題。」

Randstad 全球協作產品負責人 Roman Spantgar



報表就像由下往上的金字塔系統，層層疊加，讓各層級都安心：

用戶端加密：

加密是安全防護的基礎，但加密機制必須持續套用才能發揮作用。報表工具可確認機密資料從建立到儲存都經過端對端加密，稽核追蹤則可驗證加密金鑰仍由您控管。

情境感知存取權：

資料存取權不僅要控管，還必須監控。即時報表會顯示異常情況，例如異常存取位置、登入嘗試失敗或非上班時間的活動。有了這項功能，您就能在風險演變成事件前加以解決。

精細的存取權控管機制：

監督工具可讓您瞭解哪些人何時存取了哪些內容，以及存取目的。透過生成清楚的存取記錄和報表，您可以找出權限過高的角色、監控臨時存取權 (如支援團隊的存取權)，並遵守 GDPR 和 HIPAA 等架構。

本地資料儲存：

對於受到嚴格落地規定約束的產業來說，透明度至關重要。報表工具會驗證資料是否仍儲存在應該的位置 (無論是特定州或地區)，為 IT 團隊和監管機構提供所需證明。

資料地區：

想進軍新市場嗎？報表資訊主頁清楚顯示資料的儲存、處理和存取位置，讓企業隨著法規演進或業務擴展至全球，適時調整政策。

零信任架構：

零信任絕不假設，一律驗證。報表工具會記錄所有存取要求、裝置和使用者動作，確認無人違反資料政策，同時方便監控活動及偵測可疑的行為模式。



報表的重要性

如果沒有完善的報表功能，法規遵循工作就像在猜謎。組織必須證明自己符合法規要求，同時保持靈活，才能應對新興威脅。Google Workspace 安全控管功能提供監控工具，讓您能安心監控、驗證及調整資料策略。

- **簡化稽核作業：**生成符合法規的報表，遵守 GDPR、HIPAA 和 SOC 2 等架構。安全控管功能可簡化 IT 和法規遵循團隊的報表作業，只要按一下按鈕，就能取得所有資料活動的詳細稽核記錄。
- **全面控管：**即時資訊主頁可及早顯示風險，透明的活動記錄則會追蹤所有動作、核准或變更。團隊可掌握必要資訊，有效因應風險、證明控管成效，並維持信任關係。

安全控管功能提供即時洞察資訊、可供稽核的報表和透明的活動記錄，不僅能協助您遵循法規，還能搶先一步做好準備。有了這些監控、驗證和調整工具，組織就能自信地證明自己能控管資料，同時降低盲點或新興威脅的風險。

完善的報表功能可將法規遵循從只是交差，轉變為策略優勢。有了監控活動、驗證控管機制及主動應變的工具，組織就能自信地因應不斷變化的風險和法規，同時建立信任。





05

結語



Google Workspace 安全控管功能

結合先進的法規遵循工具與雲端的彈性和擴充性，協助組織以最少的心力，大幅提升資料主權。這項服務可精細控管資料儲存、處理和存取作業，協助企業因應不斷變化的法規。無論是保護航太業的智慧財產，還是管理金融業的客戶私密資料，安全控管功能讓組織能專注於協作、成長和創新。

[瞭解詳情](#)