公開標準與台灣產業治理觀察｜繁體中文台灣版

ISO/IEC 27701:2025 與 AI 治理標準在台灣供應鏈的應用脈絡

從 ISO/IEC 27001、27701、42001、23894、42005 到雲端與驗證制度的企業閱讀指南

C20004176 · 2026年7月2日

閱讀定位。本報告使用公開可查的 ISO/IEC 標準資訊與台灣主管機關公開資料，整理 2023-2026 年間資訊安全、隱私資訊管理、雲端 PII、AI 管理系統、AI 風險管理與 AI 影響評估的發展脈絡。本文不重製 ISO 付費標準條文，也不構成法律、驗證或投資意見；其目的在於協助台灣企業把標準語言轉譯為可被董事會、法務、資安、R&D、IPR、採購與國際客戶共同理解的治理證據。

核心結論是：企業 AI 應用已不只是一個 RAG 或聊天機器人專案，而是一組牽涉個資、商業機密、模型資料、第三方 API、跨境雲端、供應商責任與自動化決策的資料處理鏈。ISO/IEC 27001、27701 與 42001 因此應被一起閱讀：27001 管理資訊安全，27701 管理個資與隱私問責，42001 管理 AI 系統生命週期與 AI 特有風險。

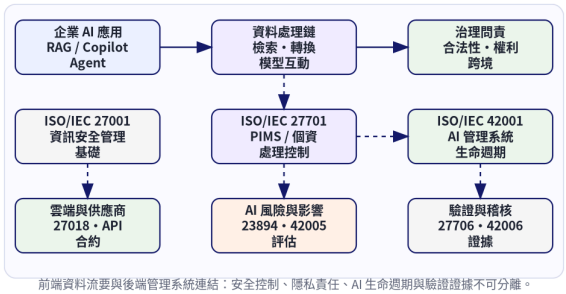
一、近期標準發展：從安全控制到 AI 與隱私管理系統

ISO/IEC 27001:2022 仍是資訊安全管理系統（ISMS）的基礎標準，公開說明將其定位為管理資訊安全風險、維持機密性、完整性與可用性的管理系統要求 [2]。對台灣企業而言，27001 的實務意義不只在於「有沒有資安證書」，而在於是否能證明人員、政策、技術、供應商、事件應變與營運流程均納入風險管理。

ISO/IEC 27701:2025 的重要變化是 PIMS（Privacy Information Management System，隱私資訊管理系統）可作為獨立管理系統使用。ISO 公開資料說明該標準用於建立、實作、維持與持續改善 PIMS，並面向 PII 控制者與處理者 [1]。這代表隱私治理不再只是資訊安全管理的附屬章節，而逐漸成為供應鏈盡職調查、資料處理合約與客戶信任的一個獨立治理層。

AI 相關標準則正在快速成形。ISO/IEC 42001:2023 是 AI 管理系統標準，適用於開發、提供或使用 AI 產品與服務的組織 [4]；ISO/IEC 23894:2023 提供 AI 風險管理指引 [5]；ISO/IEC 42005:2025 聚焦 AI 系統影響評估，協助組織識別並文件化 AI 對個人、群體與社會的可能影響 [6]。同時，ISO/IEC 42006:2025 與 ISO/IEC 27706:2025 針對 AIMS 與 PIMS 驗證機構能力提出要求，顯示第三方稽核與驗證制度正在補齊 [7][8]。

圖1　AI 應用、資料處理與 ISO 管理系統的關係圖



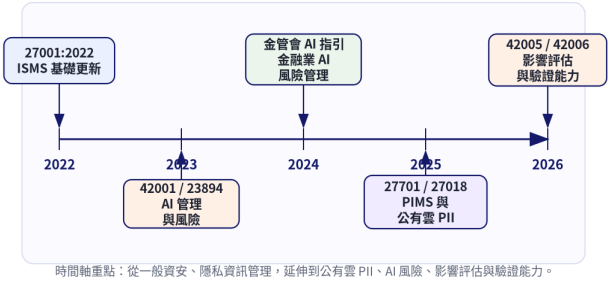
前端資料流要與後端管理系統連結：安全控制、隱私責任、AI 生命週期與驗證證據不可分離。

圖示以靜態 SVG 呈現標準群之功能關係；箭頭表示治理證據從技術控制、隱私責任到 AI 生命週期制度的連結。

表1　相關 ISO/IEC 標準在 AI 與隱私治理中的角色

標準	主要功能	對台灣企業的閱讀方式	主要讀者
ISO/IEC 27001:2022	ISMS 資訊安全管理系統	AI 基礎設施、存取控制、事件管理、供應商安全與營運韌性；屬於多數 B2B 稽核的共同語言。	CISO、IT、採購、營運
ISO/IEC 27701:2025	PIMS 隱私資訊管理系統	把個人資料處理責任制度化，釐清控制者／處理者角色、目的限制、當事人權利、資料分享與保留證據。	法務、DPO、資安、產品
ISO/IEC 27018:2025	公有雲 PII 處理者指引	針對公有雲服務提供者作為 PII 處理者的控制與原則；對台灣 SaaS、AI API 與雲端委外評估具實務關聯。	雲端架構、採購、法務
ISO/IEC 42001:2023	AIMS AI 管理系統	要求組織建立、維持與持續改善 AI 管理系統；讓 AI 風險、責任、透明度與生命週期治理可被管理。	CEO、AI 產品、R&D、稽核
ISO/IEC 23894:2023	AI 風險管理指引	提供 AI 風險管理與整合至組織活動的指引；可作為 AI 風險分級、測試與風險處置流程的參考。	R&D、資安、風險管理
ISO/IEC 42005:2025	AI 系統影響評估	聚焦 AI 系統及可預見用途對個人、群體或社會的影響評估；對 profiling、招募、金融與醫療場景特別重要。	法遵、產品、資料科學
ISO/IEC 27706:2025／42006:2025	驗證機構能力要求	分別對 PIMS 與 AIMS 驗證機構提出能力與一致性要求，代表隱私與 AI 管理系統的第三方驗證制度正在成形。	稽核、法務、治理辦公室

圖2　2022-2026 標準與台灣政策節點



時間軸重點：從一般資安、隱私資訊管理，延伸到公有雲 PII、AI 風險、影響評估與驗證能力。

時間軸顯示資訊安全、AI 管理、隱私資訊管理、雲端 PII 與台灣金融／個資政策逐步匯合；企業可用此圖安排導入優先順序。

二、為何 2026 年不能只談 RAG：AI 應用變成資料處理鏈

RAG 的主要價值是把企業文件、規格、客服紀錄或知識庫納入檢索脈絡，降低模型憑空生成的機率。可是企業 AI 落地後，實際風險不只出現在「答案是否正確」，也出現在資料是否被不當收集、提示詞是否含有個資或營業秘密、向量索引是否保留不應長期保存的資料、外部 API 是否留存內容，以及模型輸出是否造成不公平或不可追溯的決策。

因此，台灣企業在討論 AI 治理時，應把 AI 系統分成五個層次：第一是資料來源，包括內部文件、郵件、ERP、CRM、客戶服務、研發紀錄與供應商資料；第二是資料轉換，包括清理、去識別化、向量化、微調與摘要；第三是模型與工具，包括 LLM、分類器、代理工具與外部 API；第四是輸出與行動，

包括自動回覆、採購建議、風險評分、報表與 API 寫入；第五是證據，包括日誌、核准紀錄、模型版本、風險評估、事件應變與資料刪除紀錄。

在此架構下，ISO/IEC 27701 的目的限制、資料主體權利、角色責任與資料分享控制，會直接影響 RAG、Copilot、Agentic AI、Profiling 與聯邦式學習的工程設計。ISO/IEC 42001 與 23894 則使 AI 的風險分級、測試、監控、人工覆核與持續改善進入管理系統語言。這兩組標準合併後，資安團隊不能只回答「資料是否加密」，還要能回答「資料為何被處理、由誰控制、進入哪個模型、保留多久、可否刪除、是否用於再訓練、誰批准自動化行動」。

表3　超越 RAG 的 AI 應用與隱私／資安控制重點

應用型態	典型流程	主要治理風險	建議控制與證據
Agentic AI／自主工作流	AI 代理讀信、更新 CRM、呼叫 ERP/API、安排採購或排程。	資料流不易追蹤、越權存取、把 PII 或商業機密傳給第三方工具。	最小權限、工具白名單、動作審批門檻、PII 存取日誌、輸出前 DLP。
Profiling／預測分析	信用評分、客戶分群、人才篩選、語音情緒分析與風險預測。	過度推論敏感資訊、偏差、當事人不知情或無法申訴。	DPIA/PIA、模型偏差測試、人工覆核、可解釋性說明、拒絕／替代流程。
Copilot／日常辦公 AI	會議摘要、客服草稿、程式碼生成、合約或規格摘要。	提示詞含個資、客戶資料、未公開設計或專利草案；資料保留與再訓練界線不清。	企業版 AI 政策、資料遮罩、DLP、保留設定、機密資料分類與教育訓練。
Federated Learning／分散式訓練	醫院、製造據點或供應商資料不離場，但共享模型參數或梯度。	參數可能遭模型反轉或成員推論；資料品質與責任分界不清。	差分隱私、聚合安全、模型參數洩漏測試、資料治理協議。

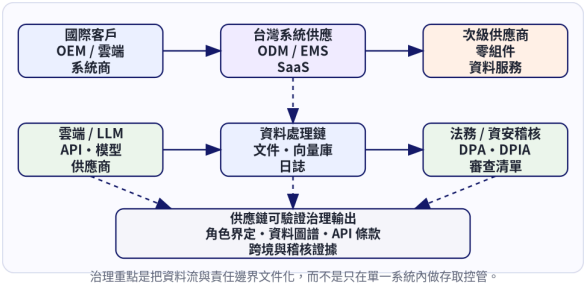
三、台灣供應鏈的影響：從證書到客戶可驗證證據

台灣企業在全球供應鏈中常同時扮演 OEM、ODM、EMS、IC 設計、模組供應商、SaaS 供應商或資料處理者。這些角色在 AI 導入後產生新的責任分界：有些企業是個資控制者，有些只是依客戶指示處理資料，有些則在多層次供應鏈中扮演次處理者或共同責任者。當國際買方要求供應商提供資安、隱私與 AI 風險證據時，單純提供一張資安證書通常不足以說明 AI 系統如何使用資料。

從採購與合約角度看，ISO/IEC 27701:2025 對台灣 SaaS、雲端、AI API、客服外包、人資系統、文件管理與資料分析服務的影響較直接，因為這些服務經常處理客戶或客戶員工的個人資料。ISO/IEC 27018:2025 又進一步補上公有雲作為 PII 處理者的保護指引，特別適用於需要評估雲端供應商資料保留、刪除、次處理者、跨境與稽核權的場景 [3]。

從主管機關脈絡看，金管會於 2024 年發布「金融業運用人工智慧（AI）指引」，公開資料指出其內容涵蓋 AI 定義、生命週期、風險評估、風險基礎落實核心原則與第三方業者監督管理 [10]。個資法部分條文修正案則已於 2025 年 11 月 11 日公布，施行日期由行政院另定，公開資料顯示修正內容包括個資事故通報、個資會職權與相關章節調整 [11]。這些本地法規與指引不等同於 ISO 標準，但會使台灣企業更需要把國際標準語言轉成可被主管機關、客戶與稽核員理解的內控制度。

圖3　台灣供應鏈中的 AI 資料流與治理證據



圖示強調台灣主承包商位於國際買方、次供應商、雲端服務與內部資料處理層之間；治理重點是把資料流與責任邊界文件化。

表4　台灣產業場景與可優先建立的治理能力

場景	AI 導入方式	標準化／法規壓力	實務起點
製造／電子供應鏈	AI 代理自動解析供應商郵件、比對交期、更新 ERP。	買方會關注：供應商聯絡個資、跨境服務、次處理者、內部人員越權、模型記憶是否外洩其他供應商資訊。	建立供應鏈資料分類、郵件解析最小化、向量庫去識別化、API 保留政策與供應商合約附件。
金融／FinTech	AI 客服、理財助理、詐欺偵測、授信預測。	台灣金管會指引已把治理、問責、隱私、客戶權益、第三方管理與風險基礎方法納入金融業 AI 管理語境。	把 42001/23894/42005 對接金管會 AI 指引；建立模型上線審查、客戶告知、人工介入與第三方 API 管理。
醫療／生技	疾病預測、臨床摘要、聯邦式學習、基因資料分析。	健康資料高度敏感；即使原始資料不離院，模型參數與摘要輸出仍需檢查是否可反推個人特徵。	PIA/DPIA、資料去識別化驗證、模型反轉測試、IRB／資料使用協議與模型版本紀錄。
SaaS／雲端／AI 工具商	為全球客戶提供 CRM、人資、客服、文件 AI 或 API。	常扮演 PII 處理者或次處理者；歐美客戶盡職調查會要求資料保留、刪除、次處理者與事件通報證據。	27701 PIMS、27018 雲端 PII、零資料保留選項、DPA、SOC/ISO 對照與稽核證據包。

四、從控制者到處理者：AI 系統設計的四個問題

ISO/IEC 27701 的實務價值，在於把隱私要求轉成可分派責任與可保存證據的管理系統。對 AI 專案而言，最容易出現落差的是角色界定、目的限制、自動化行動、資料刪除與更正。這些問題若等到產品上線後才補文件，往往會造成模型資料集、向量索引、日誌與第三方 API 設定難以回溯。因此較穩健的作法，是在 AI 專案立案時就先把資料角色與資料流納入設計審查。

控制者／處理者的界線在台灣供應鏈中尤其重要。主承包商可能只依客戶指示處理終端用戶資料，但也可能把供應商聯絡資料、員工績效資料或客服語音資料用於自身營運分析；兩者的責任與告知邏輯不同。若企業同時把資料送往境外雲端、第三方 LLM 或資料標註服務，次處理者與跨境傳輸評估也會進入客戶稽核範圍。

表6　把 27701 轉成 AI 系統設計問題

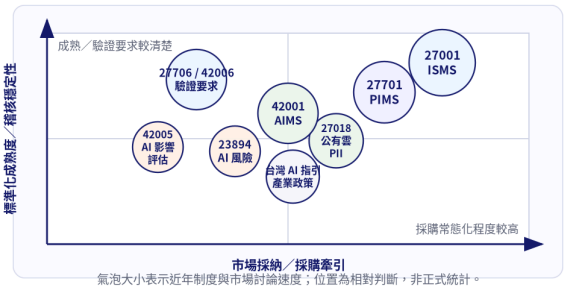
檢核面	需要回答的問題	對 AI 系統的意義	證據
角色界定	每一個 AI 系統是否已標示公司是 PII 控制者、處理者、共同控制者或次處理者？	避免把客戶資料、供應商個資與員工資料混成同一個責任邏輯。	角色判斷表、DPA、RACI
目的限制	AI 讀取文件、建立向量、摘要、微調、監控或再訓練的目的是否分開記錄？	「為了提升效率」不足以作為所有資料再利用的共同目的。	目的表、保留期間、告知文字
自動化行動	代理式 AI 是否可以直接寄信、下單、修改 ERP 或發出客戶建議？	AI 從資訊輔助變成可執行行動時，權限與覆核門檻需提高。	工具權限、審批規則、日誌
刪除與更正	當客戶或員工要求刪除／更正資料，是否能定位原始文件、向量索引、提示日誌與微調資料？	模型去學習不一定在所有場景可行，但資料集與索引的刪除流程需先定義。	資料索引、刪除紀錄、例外理由

五、標準成熟度與市場採納：不是每個標準的採購壓力相同

27001 已是較成熟的 B2B 採購語言；27701 因 2025 年版成為獨立 PIMS，採納速度可能受個資法修正、跨境資料處理、SaaS 客戶要求與歐美隱私盡職調查影響。42001、42005 與 42006 則代表 AI 管理系統、AI 影響評估與驗證能力逐步成形，但多數市場仍在把標準語言轉化為採購條款、內部稽核項目與模型上線流程。

以下圖形將標準化成熟度、買方採納成熟度與近年發展速度放在同一張相對定位圖中。此圖不代表正式市場統計，而是幫助企業決定導入順序：已成熟且買方常要求者，適合作為基線；快速發展但市場尚在形成者，適合作為 AI 新專案的設計要求與稽核準備。

圖4　標準化成熟度、採納成熟度與發展速度相對圖



氣泡大小表示近年制度與市場討論速度；位置為相對判斷，非正式統計。

本圖以 D3 風格資料點生成邏輯整理為靜態 SVG；氣泡大小表示近年制度化與採購討論速度的相對強度，兩軸為相對判斷。

六、不同公司角色如何讀這組標準

同一組標準對不同角色的意義不同。CEO　需要看治理責任與市場準入；法務需要看角色、合約與當事人權利；資安團隊需要把隱私要求落實到存取、日誌、DLP、加密與事件應變；R&D　需要把模型生命週期、資料來源與測試紀錄納入工程流程；IPR 團隊則需要避免生成式 AI 對標準提案、專利草稿、程式碼與營業秘密造成不可控的輸入輸出風險。

表2　不同公司角色的閱讀路徑與可交付證據

角色	應如何閱讀標準	可先建立的證據
CEO／總經理	把 27001、27701、42001 視為「治理能力與客戶信任證據」，而非單一證書。決策重點是範圍、優先順序、預算、責任歸屬與對外說明一致性。	AI 系統清冊、重大資料流、供應商風險、年度稽核路線圖
法務／合規／DPO	界定資料控制者、處理者與共同責任；審查 DPA、跨境傳輸、目的限制、保留期間、當事人權利與事件通報。	角色矩陣、資料處理目的表、DPIA/PIA、合約條款
資安／IT／雲端	把 27701 的隱私要求落到 27001 控制：IAM、日誌、DLP、加密、備份、事件應變、供應商存取與開發安全。	零信任政策、DLP 規則、金鑰管理、稽核日誌
R&D／資料科學	將 AI 生命週期納入設計審查：資料來源、資料品質、偏差測試、模型版本、輸出監控、人工覆核與可追溯性。	模型卡、資料卡、測試紀錄、Prompt/輸出保留政策
IPR／標準／研發法務	控管生成式 AI 對程式碼、專利草稿、標準提案與營業秘密的輸入輸出風險；確認資料來源與授權邊界。	開源／授權檢查、標準文件資料邊界、發明揭露流程

七、對資安專家的再訓練重點

過去資安訓練常把重點放在邊界防禦、漏洞修補、資產盤點與事件應變。這些能力在 AI 時代仍然必要，但不足以單獨處理隱私與 AI 管理系統。資安專家需要增加三種能力。第一是資料處理合法性與目的限制的閱讀能力，能理解個資為何被處理、是否超出原始目的、是否需要當事人告知或同意。第二是 AI 生命週期證據能力，能保存資料來源、模型版本、測試紀錄、人工覆核與輸出監控。第三是供應商與雲端合約能力，能審查資料保留、再訓練、次處理者、跨境、事件通報與稽核權。

在勒索軟體與資料外洩情境中，PIMS 的價值不只在合規，也在縮小可被勒索的資料範圍。若企業能把個資最小化、保留期間、去識別化與存取紀錄落到系統設計，攻擊者取得的資料價值與企業事件應變負擔都可能降低。這也是為什麼 27701 不宜被視為「法務文件」，而應被納入 27001 的資安控制與 42001 的 AI 管理系統之中。

表5　導入與重訓的階段式實務路線

時間	工作主軸	具體內容	輸出證據
0-30 天	盤點 AI 系統與資料流	列出所有 Copilot、RAG、API、模型訓練、客服與內部自動化工作流；標示是否涉及個資、機密、跨境、第三方或自動化決策。	AI 系統清冊、資料流圖、供應商清單
31-90 天	界定角色與責任	對每個 AI 系統標示公司是控制者、處理者、共同控制者或次處理者；對接 DPA、使用目的、保留期間與事件通報。	角色矩陣、RACI、合約缺口表
91-180 天	建立風險分級與控制基線	把 27001 的資安控制、27701 的隱私控制、42001/23894/42005 的 AI 風險與影響評估整合為一套上線 gate。	AI 風險分級、DPIA/PIA、模型測試與人工覆核紀錄
180 天以後	形成可稽核治理循環	把政策、教育訓練、日誌、事件演練、供應商審查與內部稽核固定化，必要時評估整合驗證。	管理審查紀錄、稽核報告、改善追蹤、客戶回覆包

表7　常見誤區與較穩健的修正方向

常見誤區	修正方向
把 ISO 證書等同法規合規	ISO 管理系統可提供治理框架與證據，但不能自動取代個資法、GDPR、金融監理或醫療法規判斷。
只封鎖公有 AI，不建立企業替代路徑	若缺少核准工具、DLP、資料分類與教育訓練，員工仍可能以個人帳號處理機密資料。
把 RAG 視為沒有隱私風險	向量資料庫仍可能保存可識別資訊、商業機密或可回溯文字片段；刪除、保留與權限需獨立設計。
忽略次供應商與 API 保留政策	AI 服務常牽涉雲端、模型 API、資料標註、客服外包與監控工具；合約與稽核權需延伸到次處理者。

八、IPR 與研發標準團隊的特別注意事項

AI 治理與 IPR 的交會點在於資料來源、輸入輸出與可追溯性。標準提案、專利草稿、claim　chart、程式碼、設計規格與客戶需求文件，往往同時包含營業秘密、可專利技術資訊與第三方權利資料。若員工把這些內容輸入未經核准的公有 AI 工具，風險不只在隱私，也在發明新穎性、營業秘密保護、客戶保密義務與開源授權污染。

研發與 IPR 團隊可把 ISO/IEC 42001 的 AI 生命週期管理與 ISO/IEC 27701 的目的限制合併成一份「AI　工具使用分級表」：公開資料可用於一般摘要；客戶文件與未公開標準提案需使用企業核准環境；專利草稿、claim　chart、source code 與未公開設計則需額外審查保留設定、訓練排除、存取權限與輸出保存。此做法不是把 AI 全面禁止，而是讓 AI 使用與資料機密性、個資敏感性、發明階段與合約義務相匹配。

九、結語：台灣企業應建立「一份資料流、三個管理系統」的共同語言

面對 2026 年的 AI 導入，台灣企業不宜把 ISO/IEC 27001、27701 與 42001 分別交給三個團隊各自處理。比較可行的做法，是先建立一份跨部門資料流圖，標示 AI 系統、資料來源、第三方工具、個資類型、跨境位置、模型用途與輸出行動，再把這份資料流同時映射到 27001 的安全控制、27701 的隱私責任與 42001 的 AI 生命週期治理。

對台灣供應鏈而言，這樣的整合語言具有實務價值：它可以支援國際客戶稽核、主管機關檢視、雲端供應商審查、內部 AI 上線審查、研發與 IPR 資料邊界管理。最終重點不是把每個標準都立即導入驗證，而是先把公司內部最重要的 AI 資料處理活動變成可描述、可控制、可證明與可改善的治理循環。

資料來源與參考文件

以下列出本報告引用之公開資料來源。ISO 標準全文多屬付費文本，本文僅依 ISO 官方公開摘要、標準頁面與主管機關公開資訊進行分析性整理；正式條文、控制編號與驗證要求應以購入之正式標準文本、驗證機構與主管機關要求為準。

[1] ISO/IEC 27701:2025
Information security, cybersecurity and privacy protection - Privacy information management systems - Requirements and guidance.
https://www.iso.org/standard/27701

[2] ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection - Information security management systems - Requirements.
https://www.iso.org/standard/27001

[3] ISO/IEC 27018:2025
Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors.
https://www.iso.org/standard/27018

[4] ISO/IEC 42001:2023
Information technology - Artificial intelligence - Management system.
https://www.iso.org/standard/42001

[5] ISO/IEC 23894:2023
Information technology - Artificial intelligence - Guidance on risk management.
https://www.iso.org/standard/77304

[6] ISO/IEC 42005:2025
Information technology - Artificial intelligence (AI) - AI system impact assessment.
https://www.iso.org/standard/42005

[7] ISO/IEC 27706:2025
Requirements for bodies providing audit and certification of privacy information management systems.
https://www.iso.org/standard/27706

[8] ISO/IEC 42006:2025
Requirements for bodies providing audit and certification of artificial intelligence management systems.
https://www.iso.org/standard/42006

[9] ISO AI standards overview / ISO/IEC JTC 1/SC 42 catalogue
Official public listing of published and under-development AI standards, including 22989, 23053, 38507, 5338, AI logging, de-identification and human-oversight work items.
https://www.iso.org/sectors/it-technologies/ai

[10] 金管會
金融業運用人工智慧（AI）指引與核心原則公開資料，2023-2024.
https://www.fsc.gov.tw/

[11] 個人資料保護委員會籌備處
個人資料保護法部分條文修正案於 2025 年 11 月 11 日公布，施行日期由行政院另定。
https://www.pdpc.gov.tw/News_Content/20/1010/

[12] 行政院
行政院及所屬機關（構）使用生成式 AI 參考指引公開資料。
https://www.ey.gov.tw/Page/448DE008087A1971/40c1a925-121d-4b6b-8f40-7e9e1a5401f2

附表1　企業 AI／隱私治理自評問題

檢核項	問句	主責
AI 系統清冊	公司是否知道目前所有部門正在使用哪些 AI 工具、模型 API、RAG 系統與自動化代理？	治理辦公室／IT
資料分類	輸入模型的資料是否已標示公開、內部、機密、個資、敏感個資或客戶限制資料？	資安／資料治理
供應商保留	外部 AI API 是否提供資料保留、再訓練排除、次處理者、地區與事件通報條款？	採購／法務
人工覆核	哪些 AI 輸出可直接採用，哪些必須經人工覆核或主管批准後才能對外或寫入系統？	產品／營運
刪除定位	是否能從原始文件、索引、提示日誌、訓練資料與模型版本中定位待刪除或限制處理的資料？	工程／DPO
IPR 邊界	專利草稿、標準提案、source code、claim chart 與未公開設計是否禁止輸入未核准 AI 工具？	IPR／R&D 法務
事件演練	若 AI 工具誤傳個資、外洩提示詞或產生錯誤自動化行動，是否已有通報與鑑識流程？	資安／法務
管理審查	董事會或管理階層是否定期檢視 AI 風險、重大事件、供應商變更與改善追蹤？	CEO／內稽

附表2　AI 工具分級與最低證據包

資料或任務	建議使用環境	最低證據
公開資料摘要	可使用核准工具；避免輸入未公開客戶或公司資料。	工具清單、使用政策
內部流程文件	使用企業帳號與保留設定明確的環境；必要時先去識別化。	DLP 規則、保留期間
客戶資料／個資	需確認角色、目的、告知、合約與跨境條件；預設不進入再訓練。	DPA、PIA/DPIA、API 條款
專利、source code、未公開標準提案	限企業核准封閉環境；輸出需人工覆核與授權檢查。	資料邊界、審批與輸出紀錄