KPMG

解密歐盟人工智慧法案

了解《人工智慧法案》的影響以及應對方法

KPMG make the difference.

目錄

介紹

人工智慧 (AI) 為社會和企業帶來了新的效益，其目標是改變工作場所和主要產業。簡而言之，迎接卓越發展的人工智慧和自動化之競賽已經開始。

正如KPMG《2023全球科技應用調查報告》所揭露，大多數全球高階主管(62%)表示，在過去24個月中，與人工智慧和機器學習相關的數位化轉型計劃已提升了業績或盈利能力。其中68%的受訪者表示，這些技術在未來三年內，將扮演著協助他們實現業務目標的重要角色；而有57%的受訪者認為，人工智慧和機器學習對於實現他們的短期目標來說，也可謂至關重要。

隨著人工智慧在全球商業和日常生活中普及，已迫切需要制定防範措施和法律來應對重大的新風險，像是關於如何適當且合乎道德的使用人工智慧，以及關注其發展和分布。

根據KPMG澳洲和昆士蘭大學進行的一項全球調查《Trust in artificial intelligence》顯示，有五分之三的人對信任人工智慧系統保持謹慎態度，並且有71%的受訪者希望能對人工智慧能夠進行監管。

最近，全球科技巨頭的CEO們也在美國國會山莊的一次會議上，呼籲加強人工智慧的監管，以保護人們免受人工智慧嚴重的影響。

作為回應，歐盟已就全面的《人工智慧法案》(AI Act) 達成了臨時協議。該法案採取風險管理導向的方法，保護基本權利、民主、法治和環境永續性。該法案預計將於2024年立法，並有望從2025年開始實施，而《人工智慧法案》作為此領域中首見的法律，也預計會成為全球人工智慧監管實際的新標準。

隨著《人工智慧法案》的推出，歐盟的目的是希望在促進採用人工智慧與確保人民有權利使用負責任、合乎道德和可信賴的人工智慧之間取得平衡。在本文中，我們將探討《人工智慧法案》對組織有何意義，並研究《人工智慧法案》的結構、規定的義務、合規的時程表以及組織應考慮的行動計劃。

> “組織領導層應根據《人工智慧法案》、公司品牌、價值觀和風險承受能力推動各項舉措，以促進同仁負責任地使用人工智慧，這有助於促進道德發展、監管合規、風險趨緩和利害相關人的信任。”

David Rowlands
GlobalAILeader
KPMG International

> “人工智慧的開發和使用應以安全和道德為重點，將技術進步轉化為對社會的正面力量，而歐盟《人工智慧法案》將有助於促進創新，同時能夠保護最終使用者。”

Laurent Gobbi
Global TrustedAILeader
KPMG International

執行摘要

《人工智慧法案》目標在於規範人工智慧的道德使用

人工智慧擁有巨大的前景，能夠拓展可實現目標的視野，並影響世界、造福人群，而管理人工智慧的風險以及潛在已知和未知的負面後果也相當重要。

《人工智慧法案》將於2024年定案，目標在於確保人工智慧系統安全、尊重基本權利、促進人工智慧投資、改善治理， 並鼓勵建立統一的歐盟人工智慧市場。

大多數的人工智慧系統需於2026年上半年以前開始遵守《人工智慧法案》

《人工智慧法案》對人工智慧的定義預計將是廣泛的，並且包含各種技術和系統，因此各個組織都有可能會受到《人工智慧法案》的重大影響，且大部分的管制預計將於2026年初生效。被禁止使用的人工智慧系統，必須在《人工智慧法案》生效的六個月後逐步淘汰，而管理通用人工智慧的規則，則是預計將於 2025 年初實施。

高風險人工智慧系統的提供者和使用 者面臨著嚴格的義務

《人工智慧法案》採用風險管理導向的方法，將人工智慧系統劃分為不同的風險級別：不可接受的風險、高風險、有限風險和最低風險。高風險的人工智慧系統是被允許使用的，但是需要遵守最嚴格的規範。這些規範不僅會影響使用者，還會影響所謂的人工智慧系統「供應商」。而《人工智慧法案》中的「供應商」一詞，涵蓋了人工智慧系統的開發機構，也包括開發嚴格供內部使用的人工智慧系統的組織，重要的是，組織既可以是使用者，也可以是供給者。

供應商需要確保遵守有關風險管理、資料品質、透明度、人工監督和穩健性等等的嚴格標準。

使用者有責任在《人工智慧法案》的法律範圍內，根據供應商的具體指示操作這些人工智慧系統，包括預期目的、使用案例、資料處理、人工監督和監控的義務。

通用人工智慧系統的保護機制

新的條款也被加入於應對最近新發展的通用人工智慧(General purpose AI, GPAI)模型，包括大型生成式人工智慧模型。這些模型可適用於各種任務，也可以被整合到大量的人工智慧系統中，包括高風險系統，並漸漸成為歐盟許多人工智慧系統的基礎。

考慮到人工智慧系統可以完成的廣泛任務以及其能力的快速擴展，大家一致認為GPAI系統和以其為基礎的模型必須遵守透明度的要求。此外，具備高度複雜性、功能和性能的高影響力GPAI模型，必須遵循更嚴格的規範，這會有助於降低因模型被廣泛使用而可能產生的系統性風險。

《人工智慧法案》不影響現有的歐盟法律

現有的歐盟法律及慣例，如關於個人資料、產品安全、消費者保護、社會政策和國家勞動法等，以及與產品安全有關的歐盟部門立法法案將繼續適用，遵守《人工智慧法案》並不能免除各組織在這些領域原有的法律義務。

瞭解《人工智慧法案》對組織的影響將 是成功的關鍵

組織應該花時間為他們開發及使用的人工智慧系統創建藍圖，並按照《人工智慧法案》中的定義對其風險等級進行分類。如果有任何的人工智慧系統屬於有限風險、高風險或不可接受風險的類別，他們就會需要評估《人工智慧法案》對其組織的影響，而當務之急即是儘快瞭解這些影響以及應對的方法。

研究《人工智慧法案》的影響和範圍

歐盟執委會(EC)於2021年4月提出了《人工智慧法案》草案。2023年12月時，歐洲議會、歐洲理事會和歐盟執委會已經達成了一項臨時協議，就是將《人工智慧法案》正式定為法律。

擬議的《人工智慧法案》將重塑我們對人工智慧的思考和管理方式，類似於過去幾年在資料隱私領域發生的情況。預計將於2024年正式立法的《人工智慧法案》，可能會對在歐盟境內提供人工智慧產品、服務或系統的任何企業產生立即廣泛的影響。該法律引入了歐盟人工智慧的定義，按照風險對人工智慧系統進行分類，為人工智慧系統制定了廣泛的要求和必要的保護機制，並建立了透明度的規範。

目標是什麼？

歐盟執委會希望在促進人工智慧發展和創新的同時，有效管理新興風險，這也反映在提案的目標中：

- 確保歐盟市場上的人工智慧系統是安全的，並尊重公共權利和價值觀。
- 提供法律明確性，並促進人工智慧系統的投資和創新。
- 加強治理並有效執行道德和安全要求。
- 促進單一的歐盟市場發展合法、安全、值得信賴的人工智慧，同時防止市場的分裂。

透過我們的視角來解讀：《人工智慧法案》的潛在影響

激發正面影響

- 透過監管沙盒刺激創新，中小企業可以在沒有即時監管審查的情況下測試其人工智慧系統。
- 促進標準、行為準則和認證之間的協調。
- 提高人工智慧系統的透明度。
- 為相關參與人員創造公平的競爭環境。
- 保障基本權利，並為居住在歐盟的個人提供法律明確性。

採取最佳做法

- 對您的人工智慧系統進行分類並瞭解相關風險。
- 對高風險人工智慧系統提出更嚴格的要求(強制性風險管理、資料治理、技術文件提供等)。
- 對高風險人工智慧系統進行合格的評定和上市後的監測。
- 建立有效的監管和執行機制。

管理和降低風險

- 禁止人工智慧系統中存在不可接受的風險。
- 避免侵犯基本權利。
- 防止使用影響潛意識或是不道德的技術，因為其可能會影響或扭曲個人行為，從而對該人或其他人造成傷害。
- 盡量減少可能導致不公平或不準確結果的偏見。
- 限制因年齡、殘疾、政治立場或其他因素而對弱勢群體或群體進行剝削。

為了實現這些目標，《人工智慧法案》採用了風險管理導向的方法，使其可以建立具體的最低要求，以解決與人工智慧系統相關的風險和問題，而不會過度限制或阻 礙技術的發展，也不會不合理地增加人工智慧系統提供於市場的成本。

誰會受到影響？

歐盟內外大多數的組織都在開發或使用可能符合《人工智慧法案》的人工智慧。然而，有鑑於實施期較短，組織應深入了解他們正在開發或部署的人工智慧系統，並探討它們該如何符合《人工智慧法案》的要求。

涵蓋哪些部分？

- 無論地點在何處，任何在歐盟市場上提供人工智慧系統或將其投入使用的供應商。
- 任何位於歐盟地區以外的人工智慧系統供應商，其系統的輸出可以或有意圖在歐盟境內使用。
- 位於歐盟的任何人工智慧系統供應商。
- 任何在歐盟市場上提供人工智慧系統或使其在歐盟境內可使用的進口商或經銷商。
- 將帶有人工智慧系統的產品以其名稱或商標提供到歐盟市場，或在歐盟境內提供使用的產品製造商。
- 歐盟境內的人工智慧產品和服務使用者。

哪些不包含在內？

- 專門開發或使用於軍事目的的人工智慧系統。
- 非歐盟國家的公共機構或國際組織在國際協定的框架下，與歐盟的執法或司法單位合作時使用的人工智慧系統。
- 僅作為科學研究而開發使用的人工智慧系統。
- 在提供市場或投入使用之前處於研究、測試和開發階段的人工智慧系統 (包括免費和開源的人工智慧組件)。
- 將人工智慧用於個人用途者。

與《一般資料保護規則》(GDPR) 的執行方式相同，歐盟執委會認為在歐洲市場銷售其產品的非歐洲實體，應受到與成員國類似的監管。歐盟預計將成為全球人工智慧標準的中心，可能與美國和英國有所不同。就和GDPR一樣，《人工智慧法案》也將會具有境外效力。

在您的組織中，誰將會受到影響？

管理合規性、資料治理以及人工智慧技術的開發、部署和使用的管理階層，其角色和職責會受到《人工智慧法案》的影響。除了組織中的高階職位外，董事會和各種治理委員會也可能會受到影響，因此他們應該加強發展意識和知識。

有鑑於人工智慧廣泛的定義和當前快速普及的速度，組織應採取更全面的方法。高階主管應在人工智慧系統的有目的的創新和開發、風險管理和治理方面進行合作，以達到對《人工智慧法案》的合規要求。

法案將如何執行，以及處罰是什麼？

歐盟執委會提出了一個架構，透過成立人工智慧委員會和專家小組來執行人工智慧供應商的要求，而雙方都在歐盟層面任職，並為以下負責：

- 促進與國家監管機構的有效合作。
- 提供最佳做法建議。
- 確保法規一致適用。

每個成員國將被要求成立或指定一個國家主管機構，以確保法規的實施，並維護其活動的客觀性和公正性。

歐盟擬議的法規，可能會對所有利用人工智慧巨大力量的組織產生深遠影響，而不合規的後果則取決於違規的程度，範圍可能會從限制市場准入到巨額罰款，罰款則可能從3500萬歐元或全球營業額的7%，到750萬歐元或營業額的1.5%不等，具體得取決於侵權行為和公司規模。

追蹤歐盟的立法歷程

2021年4月
歐盟執委會公佈了一項新的《人工智慧法案》提案。

2022年12月
理事會就《人工智慧法案》通過了其共同立場 (一般方法)。

2023年6月
議會通過了他們對《人工智慧法案》草案的談判立場。

2023年6月-2023年12月
最終的《人工智慧法案》談判由理事會、委員會和議會進行，並於2023年12月達成最終確定擬議規則的臨時協議。

目前的進度
最終版本預計將在2024年上半年發表。

2024年末
將對「不可接受風險」等級的人工智慧系統實施禁令。

2025年年中
將實施通用人工智慧的多項法律義務。

2026年春季
最終的《人工智慧法案》將全部生效。

何時將生效？

《人工智慧法案》中概述的大部分義務預計將於 2026年上半年生效，禁令預計在 2024 年底生效，而通用人工智慧(GPAI) 相關的義務則是預計最早將於 2025 年開始生效。

其中GPAI指的是通用功能的人工智慧系統，例如：圖像和語音辨識、音訊和影片生成、圖形識別、問答和翻譯等，這些被廣泛運用於各個預期和非預期的場景的系統，可能會被作為高風險的系統使用或被作為其他高風險人工智慧系統的組件。

揭開《人工智慧法案》的關鍵組成要素

《人工智慧法案》是一份概括性的文件，旨在幫助提供人工智慧的明確定義，從而使《人工智慧法案》在歐盟範圍內與其他歐盟法規保持一致。《人工智慧法案》的主要目標是建立一個統一、橫向的法律框架，以促進人工智慧系統的採用，同時提供高度保護以防止其有害影響。該框架有助於建立人類對於人工智慧技術的信任，並使個人和組織更有信心使用人工智慧。

定義人工智慧

《人工智慧法案》應用了源自經濟合作暨發展組織 (OECD) 最近更新的人工智慧系統之廣泛定義。雖然《人工智慧法案》的文本尚未公開，但OECD的定義如下：

「人工智慧系統是一個基於機器的系統，根據明確或隱含的目標，從收到的輸入去推斷要如何生成可以影響環境的輸出，如預測、內容、建議和決策等。不同人工智慧系統在實際部屬後的自主性和適應性水準各不相同。」

這個定義被刻意保持廣泛，以涵蓋整個範圍，從專注於單一案例的簡單技術和系統，到專注於深度學習和生成式人工智慧的高級應用。因此，**《人工智慧法案》的適用範圍比最初預期的要廣泛許多**，遠遠超出了我們近來對於先進和生成式人工智慧的理解。《人工智慧法案》的定義範圍對人工智慧系統有多項豁免，例如:用於軍事或國防目 的的人工智慧系統，以及對自由和開源系統的有限豁免。

人工智慧風險框架和要求

《人工智慧法案》定義了一個框架來理解人工智慧相關的風險，它根據人工智慧系統的潛在風險對人工智慧系統進行分類，並根據它們獲得的資料以及利用該資料採取的決策或行動將它們分為不同的類別。

歐盟的義務將根據所使用的人工智慧類別而有所不同。雖然已經就法規的上下文達成了協定，但最終文本尚未公佈，以下內容為根據公開資訊摘要了《人工智慧法案》規定的義務。

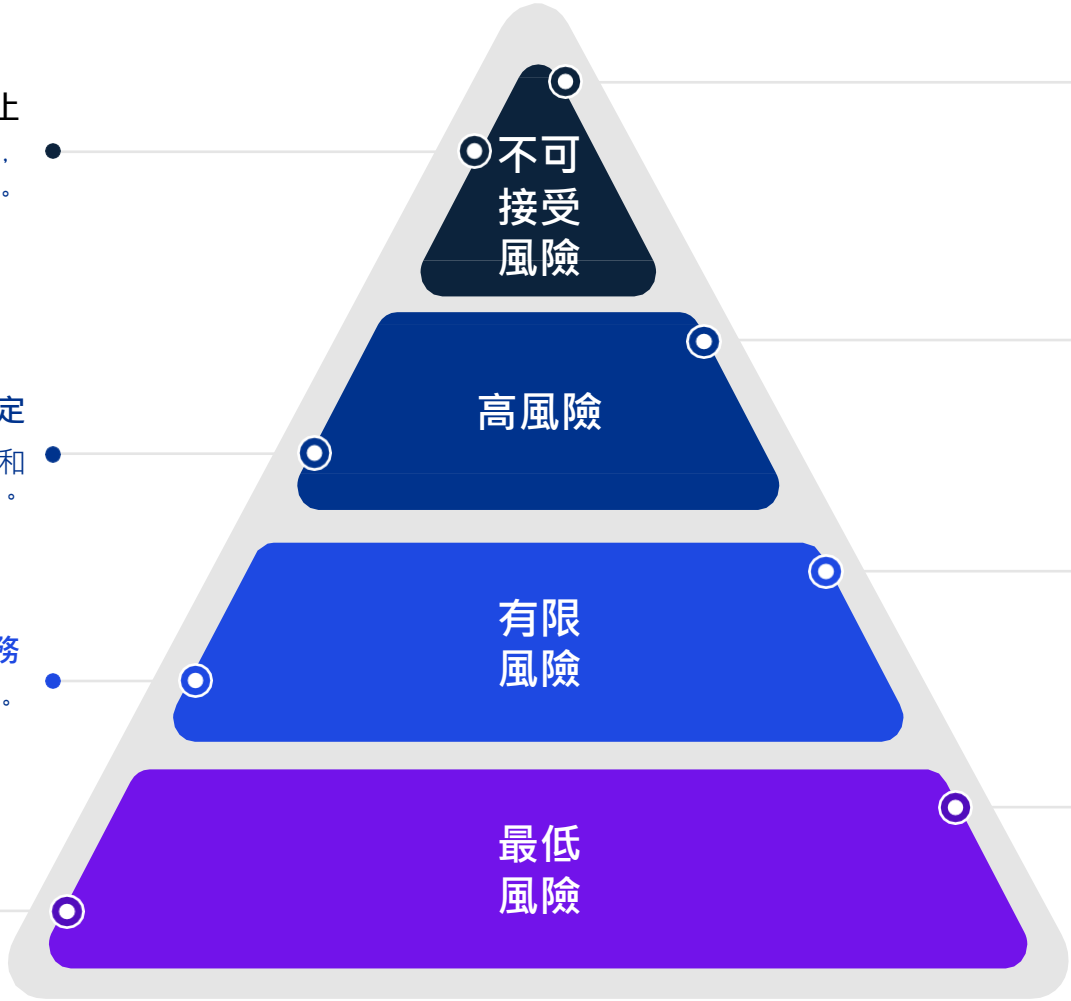
《人工智慧法案》採用以風險管理為導向的方法

禁止
違反聯盟價值觀，如基本權利。

需合格評定
對健康、安全、環境和基本權利構成高風險。

透明度義務
冒充或欺騙的風險。

無義務
沒有高風險



不可接受風險的人工智慧系統範例：
- 行為操縱
- 剝削弱勢群體
- 政府機關的社會評分系統
- 用於執法的即時遠端生物識別系統

高風險人工智慧系統範例：
- 評估獲得信貸、健康、人壽保險或公共福利的資格
- 分析工作申請或評估候選人
- 產品安全零組件

有限風險人工智慧系統範例：
- 與消費者互動的人工智慧系統。
- 生成式人工智慧*：生成或操縱內容(圖像、音訊或 影片) 的人工智慧系統。

最低風險人工智慧系統範例：
- 垃圾郵件過濾器。
- 支援人工智慧的電玩遊戲。

* 生成式人工智慧和基礎模型的進一步具體義務將適用於這種以風險為基礎的方法之外。

不可接受風險的人工智慧系統

哪些人工智慧系統涵蓋在內？

支援操縱、剝削和社會控制的人工智慧系統被視為不可接受的風險。此類別禁止出於以下目的而被使用的人工智慧：

- 傷害或可能傷害人工智慧使用者或其他人的操縱行為。
- 剝削特定弱勢族群。
- 社會評分導致自然人在社會環境中受到有害或不利的對待。
- 隨意擷取臉部影像。
- 工作場所和教育機構當中的情緒識別軟體 (有一些例外)。
- 使用人工智慧，根據種族、政治觀點或宗教信仰等敏感特徵對人進行分類。
- 對個人進行預測性警察活動 (根據個人特徵對未來犯罪進行風險評分)。
- 對人員進行遠端生物識別 (部分禁止，有一些執法部門為例外)。

與此類別相關的法律義務是什麼？

由於此類人工智慧系統構成不可接受的風險，因此被禁止使用。

高風險人工智慧系統

哪些人工智慧系統涵蓋在內？

對安全或基本權利產生負面影響的人工智慧系統將被視為高風險，並被分為兩類：

1) 用於符合歐盟產品安全指令產品的人工智慧系統，包括玩具、 航空、汽車、醫療設備和電梯。

2) 屬於特定領域且必須在歐盟資料庫中註冊的人工智慧系統，這些系統包括：

- 關鍵基礎設施，如公用事業的供應。
- 教育和職業培訓，如考試自動評分。
- 就業、工人管理和取得自營工作機會，如自動招聘和申請分類。
- 獲得基本的私人和公共服務及福利(如醫療保健)、自然人的信用評估以及與人壽和健康保險相關的風險評估和定價。
- 可能干擾基本權利的執法系統，例如針對潛在犯罪者的自動風險評分、深度偽造檢測軟體和證據可靠性評分。
- 移民、庇護和邊境管制管理，例如，核實旅行證件的真實性以及簽證和庇護申請審查。
- 司法行政和民主程序，例如協助司法機關的法律解釋工具。

大多數組織都使用這些高風險的人工智慧系統，例如：用於招募的人工智慧。

同樣重要的是要注意，執委會可以通過授權行為為高風險人工智慧系統類別增加更多用途。本報告的「後續步驟」部分對此進行了進一步討論。

與此類別相關的法律義務是什麼？

由於此類別中的人工智慧系統被認為是高風險的，因此它們將受到最嚴格的監管要求：

- 充分的風險管理，以識別、評估和減輕人工智慧系統生命週期中的風險。實際上，這項義務要求實施專門的風險管理系統，並將完成的風險評估記錄在案，且該機制需持續運作與更新。
- 適當的資料治理和管理實踐 (訓練、驗證和測試)，以確保資料集的品質。為了確保資料集不會導致歧視或不準確的結果，這將是一項關鍵的義務。值得注意的是，除非能確保輸入和輸出都不具有歧視性，否則敏感的個人資料不得包含在內。
- 技術文件必須呈現其義務遵守，並允許進行合規性評估。
- 記錄事件，以確保系統運行的可追溯性。
- 保存有關追蹤和監測高風險情況的記錄、確認記錄符合標準， 並確保人工智慧系統的輸出不會導致任何歧視性影響。
- 最低限度的記錄必須包括使用方式、資料和人員識別。
- 在歐盟高風險人工智慧系統資料庫中註冊。

- 透明度規範，使人工智慧能夠正確的詮釋和使用，並附上適當的數位格式說明。
- 實施適當的人為監督。
- 具備一定程度的的準確性、穩健性和網路安全性。

高風險人工智慧系統將接受合格評鑑，以確定它們是否符合《人工智慧法案》的要求。作為供應商，將其提供於市場前的最後一步是必須簽署合格性聲明，且人工智慧系統必須貼上CE 的合格認證標誌，以確認符合歐洲標準。 然而，這些標準的具體內容皆有待闡釋。

一旦人工智慧系統上市，將應用上市後監測的義務，包括向相關市場監督部門報告高風險人工智慧系統的故障或嚴重事件 。

部署人員的義務是什麼？

高風險人工智慧系統的部署者，包括提供基本服務的公共機構和私人企業，如銀行、保險公司、醫院和學校，都有確保負責任使用的具體義務。這些義務包括：

- 在部署人工智慧系統前完成基本權利影響評估 (Fundamental Rights Impact
- Assessment, FRIA)。
- 由受過培訓的人員進行人工監督。
- 確保輸入的資料與系統的預期用途相關。
- 在發生國家級風險時暫停系統使用。
- 向人工智慧系統供應商報告嚴重事件。
- 保留自動生成的系統紀錄。
- 如果使用者是公共機構，則需遵守註冊要求。
- 遵守 GDPR 對資料保護影響評估的義務。
- 驗證對《人工智慧法案》的遵守情況，並確保所有相關文件都可以取用。
- 告知使用者高風險人工智慧的潛在用途。

進口商和分銷商在將高風險人工智慧系統推向市場之 前，需共同承擔合規性驗證和相關訊息記錄的責任，並與供應商和市場監督機構進行溝通。

通用人工智慧、基礎模型和生成式人工智慧

哪些人工智慧系統涵蓋在內？

通用人工智慧 (GPAI) 和基礎模型在最初的提案中並沒有被定義，但已被納入當前版本，以解決人工智慧系統服務於各種目的或被整合到其他高風險系統中的情況。

- GPAI系統旨在執行普遍適用的功能，如圖像/語音辨識、音訊/影片生成、圖形識別和其他應用。著名的例子包括 ChatGPT 和 Dall-E 等等。
- 基礎人工智慧模型在廣泛的資料上進行大規模訓練，專為輸出的通用性而設計，並且可以適應各種任務。一個著名的例子是 GPT-4，它是最新版ChatGPT 下的基礎模型。

與此類別相關的義務是什麼？

GPAI系統必須符合透明度要求。其中包括提供技術文件、遵守歐盟版權法以及提供有關人工智慧訓練資料的資訊。

更強大的基礎模型將適用於更嚴格的義務。供應商必須進行模型評估、減輕系統性風險，也須進行對抗例測試(adversarial testing)、向委員會報告嚴重事件，並確保網路安全和能源效率。

單獨監管此類人工智慧系統的基本原理是供應鏈動態：基礎模型可能繼續成為下游人工智慧「提供者」和人工智慧「使用者」的重要來源，他們將這些模型使用於更具體的應用。由於這些下游用戶缺乏對基礎模型供應商的控制和議價空間，因此該法案要求模型的供應商承擔特定的監管責任。這也是我們會在報告的「後續步驟」部分討論的領域。

有限風險的人工智慧系統

哪些人工智慧系統涵蓋在內？

一些旨在與自然人互動或生成內容的人工智慧系統不一定符合高風險人工智慧系統的條件，但可能帶有身分冒充或欺騙的風險，包括大多數生成式人工智慧系統的輸出。在實務中，以下人工智慧系統被歸在此類別：

- 聊天機器人，例如基於 ChatGPT 的系統。
- 情緒識別系統。
- 生物辨識分類系統。
- 生成「深度偽造」內容的系統。

與此類別相關的義務是什麼？

此類人工智慧系統受透明度義務的約束。與廣義上影響發展和風險管理的高風險系統不同，有限風險系統的義務側重於產出和使用者：

- 必須告知人們他們正在與人工智慧系統互動。
- 接觸 (非禁止的) 情緒識別或生物識別系統的人必須被告知該系統的存在。
- 深度偽造內容必須被揭露是人為生成或人為操縱的內容。

最低風險的人工智慧系統

哪些人工智慧系統涵蓋在內？

《人工智慧法案》沒有定義這一類別。它包括不屬於其他類別的人工智慧系統，例如支援人工智慧的電玩遊戲或垃圾郵件過濾器。

與此類別相關的義務是什麼？

除了遵守一般產品安全標準外，此人工智慧類別將不受嚴格義務的約束。儘管如此，仍強烈鼓勵建立其行為準則，以促進在歐盟內被更廣泛地採用。

後續步驟

因為《人工智慧法案》的商定文本待歐洲議會和歐洲理事會通過就能正式成為歐盟法律，組織可以主動開始為合規做準備。

第一步是確保組織中的合適人員儘快開始為這些即將到來的法規要求做準備，儘早參與可讓您有更多時間瞭解需求及其對整個人工智慧生命周期的影響。《人工智慧法案》確定了各種角色，包括法律、隱私、資料科學、風險管理和採購專業人員，故負責遵守《人工智慧法案》的工作小組應涵蓋全方位的專業知識。

第二步是全面瞭解組織中開發或使用的人工智慧系統， 並根據《人工智慧法案》中定義的風險等級對其進行分類。如果您的任何人工智慧系統屬於最低、高或不可接受的風險類別，您可能需要在 2026 年前或更早之前對具有不可接受風險的人工智慧系統進行重大更改。至關重要的是，必須儘快制定明確的計劃，以管理必要的組織轉型，並確保在新的法律框架生效時及時遵守。

以下列出了您的組織可以立即和長期採取的關鍵行動，以確保可持續遵守人工智慧監管領域的當前法規和未來發展。

短期內的關鍵行動

01 定義適當的治理

- **定義策略以確定人工智慧系統的風險級別**：確定如何根據《人工智慧法案》中概述的風險類別對人工智慧系統進行分類。值得注意的是，《人工智慧法案》中被禁止和高風險的人工智慧系統清單可能會擴大。為避免代價高昂的補救措施，您的政策應考慮以下類別背後的立法理由：
  - i. 被禁止的人工智慧系統可能幫助操縱、剝削和社會控制行為
  - ii. 高風險人工智慧系統可能對歐盟裡個人的健康、安全和基本權利產生重大的負面影響。
- **管理利害關係人的期望**：與所有利害關係人 (包括客戶和合作夥伴) 進行透明的溝通，讓其瞭解您的公司如何滿足《人工智慧法案》的要求，並向每個利害關係人群體概述在管理持續合規性方面的期望和要求。
- **實施 (或改進) 您的人工智慧治理框架**：根據《人工智慧法案》的要求和其他新興監管標準，實施人工智慧系統開發、 部署和維護，以確保一致性和可擴展性。同樣地，利用自動化解決方案以協助管理法規遵循、義務追蹤和工作流程管理等方面。
- **建立永續的資料管理實務**：實施和維護強大的資料治理框架，以確保長 期的資料品質、安全性和隱私性，並靈活應對未來的技術和監管變化。

02 瞭解您的風險

- **充分確定人工智慧風險的優先順序並對其進行管理：**瞭解人工智慧系統在內部和外部對公眾、您的組織、利害關係人和整個生態系統構成的風險。這包括瞭解基本權利影響評估和系統性風險評估涵蓋的內容 (在相關範圍內) 。審查並在必要時更新您的資料處理作業，以確保它們符合適用的法律、法規和行業良好慣例， 包括資料隱私和安全。

- **對當前的人工智慧環境進行盤點和分類：**審查現有的人工智慧系統和用例，並對其進行分類，以辨別需要遵守《人工智慧法案》的高風險系統。利用自動檢測和識別解決方案，例如自動輸入問卷或實施工作流程平臺，以加速支援和遵循合規義務所需的披露、盤點和分類活動。

- **進行差距分析：**進行徹底的差距分析，以辨別不合規的領域，並制定計劃來解決這些差距。根據既定的治理框架或《人工智慧法案》合規義務，可以使用自動或快速的人工智慧評估方法加快分析。

- **徹底測試人工智慧系統：**為了確保人工智慧系統能夠按預期運行，《人工智慧法案》還建立了一個用於測試的監管沙盒。利用自動化威脅檢測、分析和智能解決方案，可以大大減少支援《人工智慧法案》中提到的測試和技術文件要求所需的工作量。

- **定義第三方風險管理流程：**增強第三方風險評估，以涵蓋特定的人工智慧考量因素。如果您的組織使用基礎模型來開發更具體的應用程式，則應持續監控這些供應商打算如何遵守 《人工智慧法案》。確定他們將提供哪些技術文件，將使您能夠管理風險和下游對您的影響。這些供應商可能會制訂更嚴格的「可接受使用」策略，以避免其GPAI模型被用於風險評估以外的目的。

03 啟動需要規模化方法的行動

- **自動化系統管理和評估：**優化、自動化和簡化人工智慧系統管理流程，確保模型是透明、可解釋和可信任的。利用自動化從人工智慧系統和應用程式元資料中提取技術指標和資料，並將其標示到您的治理框架，從而實現自動化的合規性和管理流程。

- **記錄和保存記錄：**建立文件儲存庫和管理系統，以確保文件流程到位，並確保人工智慧系統有被詳實記錄且符合《人工智慧法案》。

- **對員工進行人工智慧道德和合規方面的培訓：**就人工智慧系統的法律和道德影響以及預期用途對員工進行教育，確保他們準備好處理新的職責和合規任務。

- **消費者條款和條件**：在與消費者一起使用人工智慧系統時，請考慮是否：

  i. 需要更改您的條款和條件、隱私政策和同意聲明

  ii. 制定您的「可解釋性」聲明，使消費者能夠瞭解您的人工智慧系統的決策過程。

中長期的關鍵行動

01 預測法規對您業務的影響

- **通過透明度建立消費者信任：**優先考慮人工智慧運營的透明度，以建立和維護公眾信任，確保人工智慧解決方案的長期可行性和接受度。
- **戰略性地與監管變化保持一致：**使您的業務戰略與不斷發展的人工智慧監管環境保持一致， 並預測《人工智慧法案》未來的修訂。
- **合作並保持開放對話：**參與和人工智慧監管相關的行業討論和政策制定過程，以影響並保持領先於未來的監管趨勢。

02 發展倫理和治理

- **優先對人工智慧倫理和治理進行長期投資：**建立專門的人工智慧倫理和治理團隊或部門， 根據監管要求持續監控和指導人工智慧實務。
- **保持持續的人工智慧素養和培訓計劃：**制定長期的培訓計劃以提高整個組織的人工智慧素養，並培養合乎倫理的人工智慧使用與合規文化。

03 在創新、設計和控制中嵌入可信任的 人工智慧

- **在倫理範圍內進行創新：**營造一個尊重倫理界限和監管要求的創新環境，在技術進步與社會責任之間取得平衡。
- **通過設計實施可信任人工智慧和人工智慧安全：**調整人工智慧系統的構建，在設計階段將可信任人工智慧和人工智慧安全納入其中。
- **定期審核和更新人工智慧系統：**對人工智慧系統進行定期審查和更新，以確保持續的合規性，並整合人工智慧透明度和可解釋性方面的進步。

這與我們的工作有何關聯

我們相信人工智慧的變革力量，只有當它與人類的專業知識、獨創性和有效的風險管理相結合時，它才能充分發揮其潛力。

在KPMG，我們的目標是激發信心並推動變革。追溯我們的起源至150多年前，KPMG的員工在利用新技術以及為實施新技術提供保證和指導方向方面佔據主導角色。

透過將深厚的行業專業知識和流程知識與領先的技術聯盟相結合，KPMG的專業人士正在透過人工智慧促進價值，並為世界各地的客戶、人員和社區帶來改變。

《人工智慧法案》的許多方面對組織來說都將具有挑戰性，特別是在人工智慧應用程序的測試、透明度和可解釋性的技術文件方面。除了這一挑戰外，每個人工智慧應用程式都有自己的業務流程、影響和風險。

KPMG的專業人員可以幫助您簡化合規流程，並讓您成功應對《人工智慧法案》帶來的挑戰。我們的團隊可以實施和擴展您的人工智慧治理、管理和監控計劃，同時和您分享從先前的合作和從我們自己的人工智慧自動化旅程中學到的關鍵知識，以幫助您改進流程和政策。

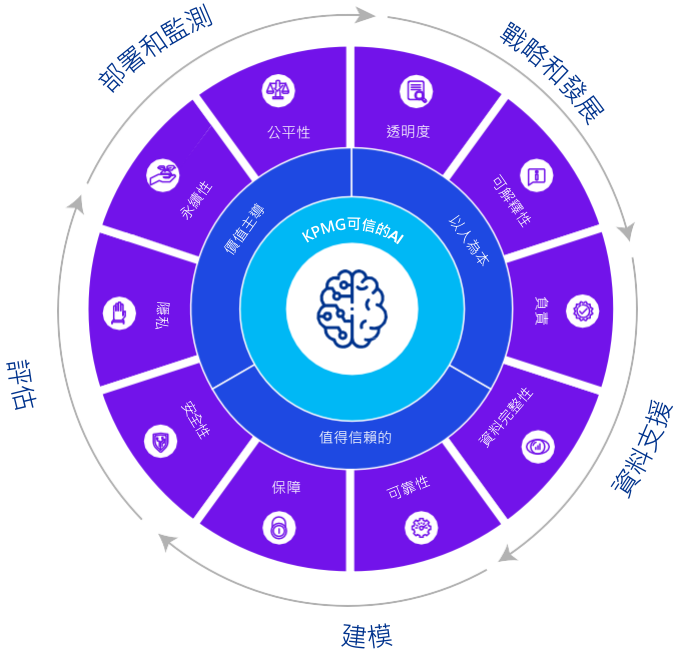
KPMG可信的人工智慧

KPMG可信的人工智慧是我們的戰略方法和框架，旨在以負責任與合乎道德的方式設計、構建、部署和使用人工智慧解決方案，以便我們充滿信心地加速實現價值，而這是基於我們在人工智慧風險管理方面的豐富經驗和現有的全球標準開發而成的。

這個多方面的框架涵蓋了營運業務線、合規線和內部審計，整合了人工智慧解決方案、治理和評估方面的廣泛專業知識。採用控件和工具設計，以幫助建立可信賴且合乎道德的人工智慧系統評估、設計和部署。

我們提供了一種廣泛的方法，使您的組織能夠有效地管理這些即將到來的監管變化。通過我們的服務，我們將協助您開始進行轉型與合規之旅，並根據您的業務需求進行客製化。

想瞭解更多資訊，請至：kpmg.com/trustedai



在地觀點

隨著全球數位與AI的生態系統逐漸成形，各國政府與企業皆針對 AI 與數位法規相關的討論相當熱絡，未來監管的趨勢也會影響企業的跨國營運與產品開發方針。人工智慧帶來的變革力量前所未見，雖然潛力無窮但企業管理者仍要認清技術的本質是「為人所用」。只有當它與人類的專業知識、獨創性和有效的風險管理相結合時，它才能充分發揮其潛力。

對於台灣企業而言，這代表我們的數位轉型必須要更加掌握中後台的數據。從數據治理先開始著手，盤點清楚數據是否有被妥善的儲存、分析、利用才能真正解構 AI 模型的黑盒子，致力於提升模型的可信任度、可解釋度與確保倫理風險不會發生。確保所有利害關係人與客戶的利益都能被保障，也才能真正讓企業的服務與品牌被深化與提升價值。

賴偉晏 Wayne Lai

KPMG 安侯建業 數位長

在地觀點

歐盟AI法案如同過去GDPR般對臺灣產業影響深遠，臺灣企業需特別關注資料保護和AI倫理。這將讓臺灣與歐盟的標準直接對接，以確保AI技術的開發和應用符合歐盟要求。同時，臺灣應把握機會，通過創新和研發，鞏固在AI領域的領導地位。此外，透過加強教育和培訓，提升專業人才在資料保護和AI合規性方面的知識和技能，也是目前產業迫切需要的。

另外，隨同AI法案發布，顧問及法律服務領域預期將迎來新的業務機會，以協助企業符合AI法案。臺灣企業若能順利接軌歐盟AI法案，不僅能在全球市場中獲得競爭優勢，亦能促進與歐洲的民間企業合作，共同推動負責任的AI技術發展。

林大馗 Toni Lin

KPMG 安侯企管
執行副總經理

KPMG
Digital Village

我們的願景

To Be the Clear Choice

在KPMG 我們自詡為「最有溫度的數位轉型推手」，陪伴企業走過數位創新的每一個環節與挑戰。

我們也希望透過這樣的方式，能協助企業高階管理者能夠看清全貌、擘劃策略。因此我們發展出完整的方法論與落地的執行方案，協助企業成功轉型。

Contact us

賴偉晏 Wayne Lai
數位長
T: +886 2 8101 6666 ext. 16208
E: wlai1@kpmg.com.tw

林大馗 Toni Lin
顧問部 執行副總經理
T: +886 2 8101 6666 ext. 15320
E: tonilin@kpmg.com.tw

李祖康 James Li
顧問部 副總經理
T: +886 2 8101 6666 ext. 13554
E: jamesli1@kpmg.com.tw

本文所提及之一部分或全部服務，依相關獨立性規範，可能無法對KPMG之審計客戶及其關係企業提供服務。

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/tw

Document Classification: KPMG Public