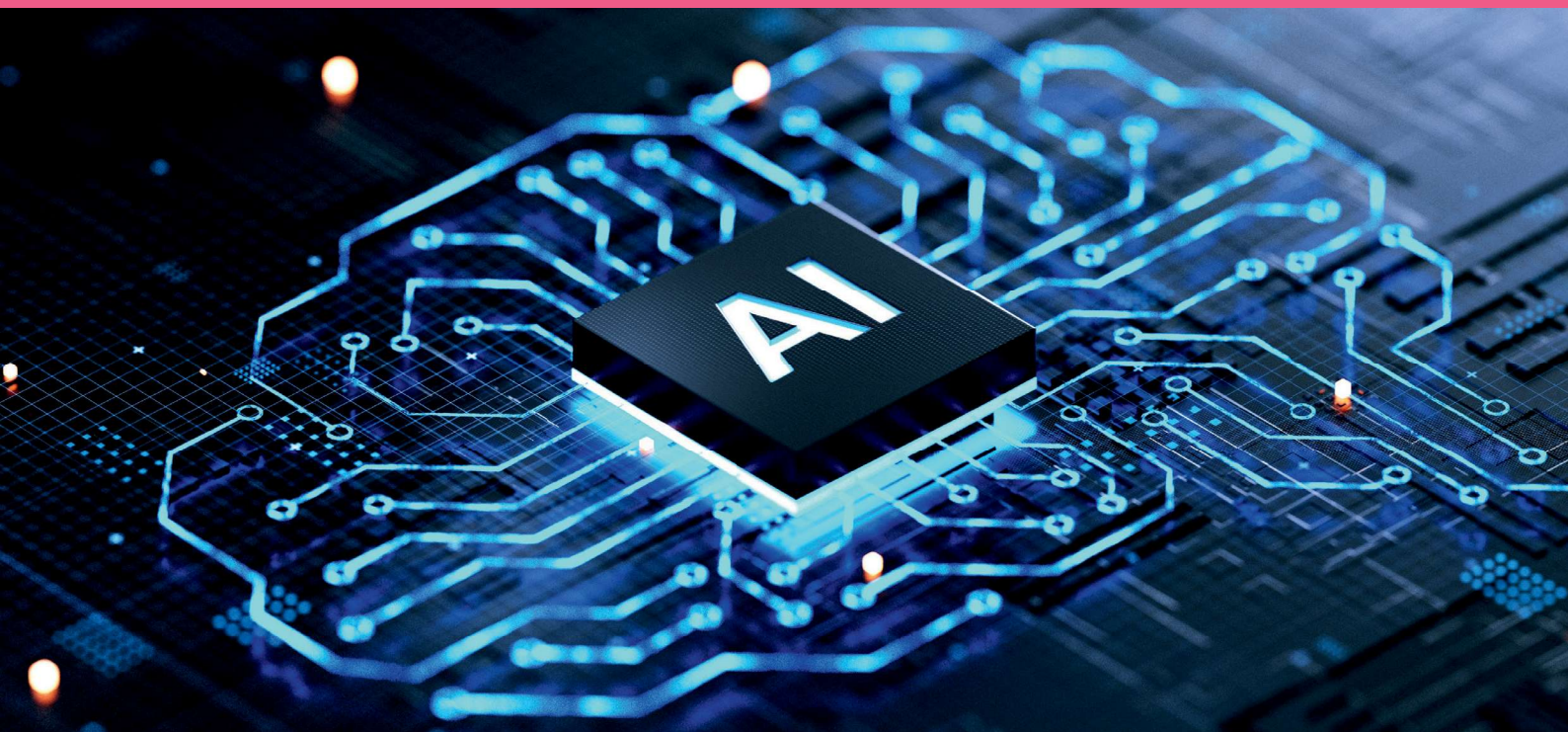


迎接AI治理新時代

解析人工智慧基本法

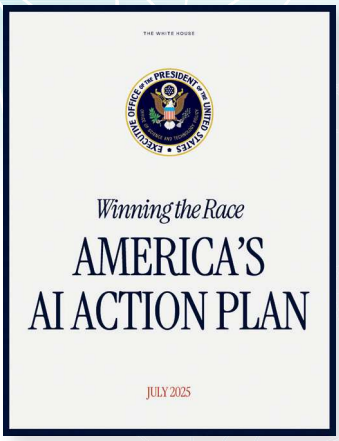
◎ 李志強／經濟部智慧財產局政風室主任

人工智慧（Artificial Intelligence, AI）技術已成為全球產業轉型與國家競爭力的關鍵驅動力，但伴隨AI技術快速發展，對個人隱私、資訊安全、社會公平甚至是國家主權均產生風險與挑戰，促使許多法治國家採取立法行動，如經濟合作暨發展組織（OECD）早在2019年即通過《人工智慧建議書》（OECD Recommendation on Artificial Intelligence），提出基本價值原則，並提供各國制訂相關政策之建議，同年歐盟發布《可信賴人工智慧倫理準則》（Ethics Guidelines for Trustworthy AI），確保

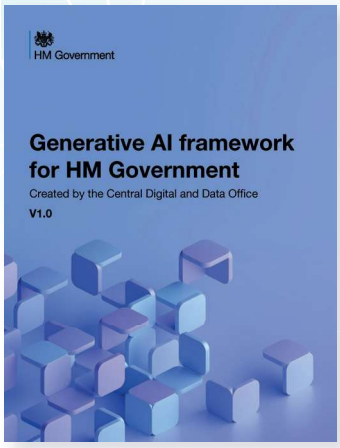
經濟合作暨發展組織（OECD）早在2019年即通過《人工智慧建議書》，提出基本價值原則，並提供各國制定相關政策建議。Photo Credit: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

人工智慧發展所需之共同倫理原則，並於2024年審議通過《人工智慧法》（Artificial

歐盟《可信賴人工智慧倫理準則》（Ethics Guidelines for Trustworthy AI）。Photo Credit: https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html

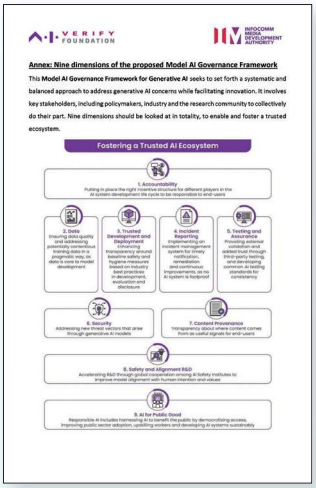


美國《AI行動計畫》（AI Action Plan）。Photo Credit: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf



英國《生成式人工智慧治理框架》（Generative AI Framework）。Photo Credit: https://www.gov.uk/government/publications/generative-ai-framework-for-hmg

Intelligence Act），美國亦於同年發布《AI行動計畫》（AI Action Plan），英國則頒布《生成式人工智慧治理框架》（Generative AI Framework）。亞洲國家如新加坡於2024年公布《生成式AI治理架構》（Model AI Governance Framework for Generative AI），日本於2025年通過《人工智慧相關技術研究開發及活用推進法》（Act on the Promotion of Research, Development, and Utilization of AI-Related Technology）、韓國頒訂《人工智慧發展及建立信任基本法》（Basic Act on the Development of Artificial Intelligence and the Establishment of Trust），由上可見建構AI法制確屬世界趨勢。



新加坡《生成式AI治理架構》（Model AI Governance Framework for Generative AI）。Photo Credit:https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/public-consult-model-ai-governance-framework-genai

日本《人工智慧相關技術研究開發及活用推進法》（Act on the Promotion of Research, Development, and Utilization of AI-Related Technology）。Photo Credit: https://www.gov-online.go.jp/hlj/en/november_2025/november_2025-08.html

法案重點

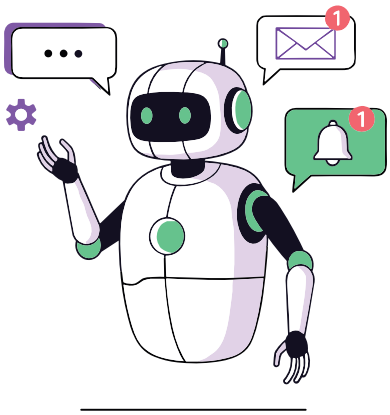
立法院於民國114年12月23日三讀通過《人工智慧基本法》（共20條），不僅是首部AI專法，也是我國邁入AI治理新紀元之關鍵，為協助社會各界掌握本法重點，以下綜整法條及立法說明歸納如下：

一、立法宗旨目的

從第1條可知，本法制定目的係為建設智慧國家，促進以人為本之人工智慧研發與產業發展，開宗明義將AI定位為驅動國家發展與提升競爭力之核心動力，並兼顧人權保障。

二、主管機關權責

第2條規定中央主管機關為國家科學及技術委員會，地方為直轄市、縣（市）政府，本法所定事項，涉及各目的事業主管機關職掌者，由各目的事業主管機關辦理。另因考量AI涉及之層面廣泛，需由行政院跨部會規劃協調，故於本法第6條明文，行政院應成立國家人工智慧戰略特別委員會（幕僚作業由國家科學及技術委員會辦理），由行政院院長召集學者專家、人工智慧相關民間團體及產業代表、政務委員、相關機關首長或代表、直轄市及縣（市）政府首長組成，協調、推動及督導全國人工智慧事務，並訂定國家人工智慧發展綱領。委員會每年至少召開會議1次，並審議國家人工智慧發展綱領；遇突發緊急或重大事件，應召開臨時會議。



三、界定AI定義

第3條明定本法所稱人工智慧，指具自主運行能力之系統，該系統透過輸入或感測，經由機器學習及演算法，可為明確或隱含之目標實現預測、內容、建議或決策等影響實體或虛擬環境之產出，此主要是參考美國、歐盟等規範。

四、揭示遵循原則

為兼顧促進AI發展與因應可能風險，第4條規定政府推動人工智慧之研發與應用，應在兼顧社會公益、數位平權、促進創新研發與強化國家競爭力之前提下，發展良善治理與基礎建設，並遵循下列七大原則：

（一）永續發展與福祉：應兼顧社會公平及環境永續，提供適當之教育及培訓，降低可能之數位落差，使國民適應人工智慧帶來之變革。

（二）人類自主：應以支持人類自主權、尊重人格權等人類基本權利與文化價值，並允許人類監督，落實以人為本並尊重法治及民主價值觀。

（三）隱私保護與資料治理：應妥善保護個人資料隱私，尊重企業營業秘密，避免資料外洩風險，並採用資料最小化原則；同時在符合《憲法》隱私權保障之前提下，促進非敏感資料之開放及再利用。

（四）資安與安全：人工智慧研發與應用過程，應建立資安防護措施，防範安全威脅及攻擊，確保其系統之穩健性與安全性。

（五）透明與可解釋：人工智慧之產出

應做適當資訊揭露或標記，以利評估可能風險，並瞭解對相關權益之影響。

（六）公平與不歧視：人工智慧研發與應用過程中，應盡可能避免演算法產生偏差及歧視等風險，不應對特定群體造成歧視之結果。

（七）問責：應確保承擔相應之責任，包含內部治理責任及外部社會責任。

五、保護相關權益

本法於第5、14及15條分別規範政府應保護人民之相關權益，說明如下：

（一）保障人民權益：政府應避免人工智慧之應用，有侵害人民生命、身體、自由或財產，破壞社會秩序、國家安全或生態環境，或偏差、歧視、廣告不實、資訊誤導或造假等違反相關法規之情事。政府應以兒少最佳利益為原則，人工智慧產品或系統經中央目的事業主管機關會商數位發展部認定為高風險應用者，應明確標示注意事項或警語。

（二）促進個資保護：各目的事業主管機關會商個資保護主管機關，在人工智慧研發及應用過程，避免不必要之個資蒐集、處理或利用，並應促進個資保護納入預設及設計相關措施或機制，以維護當事人權益。

（三）確保勞工權益：政府應積極運用人工智慧確保勞動者之勞動權益，並積極弭平人工智慧發展所造成之技能落差，提升勞動參與，保障經濟安全，並落實尊嚴勞動。另就人工智慧利用所致之失業者，依其工作能力予以輔導就業。

六、明定政府義務

本法於第7至13條及18條臚列政府應行義務，說明如下：

（一）提升國民知能：為提升國民對於人工智慧之知識與技能，政府應持續推動各級學校、產業、團體、社會及公務機關（構）之人工智慧與倫理教育，並厚植國民之數位素養，此參考《科學技術基本法》第22條所定。

（二）鼓勵產官學界：政府應落實人工智慧發展政策，並鼓勵產官學界，積極推動人才及技術之跨域合作、交流與基礎設施之建立。

（三）寬列預算經費：政府應於財政能力範圍內，寬列預算，採取必要措施，持續確保經費符合推行人工智慧政策發展所需。

（四）積極推動AI：政府應積極推動人工智慧研發、應用及基礎建設，妥善規劃資源整體配置，並辦理人工智慧相關產業之補助、委託、出資、

投資、獎勵、輔導，或提供租稅、金融等財政優惠措施，並應設置年度執行成效報告制度，定期對外公布相關成果與評估意見，以作為政策持續推動與資源調整之依據，此參酌《產業創新條例》第9條及《科學技術基本法》第6條而定。

（五）建構完善措施：政府應於人工智慧開發、訓練、測試及驗證新興技術運作之影響時，提供合理使用、扶持及補助措施，並完善人工智慧研發及應用之法規。相關法規之解釋與適用，如與其他法規扞格，在符合本法第4條基本原則之前提下，以促進新技術與服務之提供為優先原則。另為促進人工智慧技術創新及永續發展，各目的事業主管機關得針對人工智慧創新產品或服務，建立或完備人工智慧研發及應用服務之創新實驗環境。

（六）推動合作事宜：政府應致力推動人工智慧相關之國際合作；並基於公私協力原則，積極與民間共同推動人工智慧之創新運用，此參據《科學技術基本法》第21條制定

（七）資料開放共享：政府應建立資料開放、共享及再利用機制，以提升人工智慧使用資料之可利用性，並定期檢視與調整相關法令及規範。另應致力提升我國人工智慧使用資料之品質與數量，確保訓練及產出結果足以展現國家多元文化價值與維護智慧財產權。

（八）檢討法規措施：政府應依本法規定，檢討所主管之法規與行政措施；有不符合本法規定或無法規可適用者，應自本法施行後2年內，完成法規之制（訂）定、修正或廢止，及行政措施之改進。前項法規制（訂）定或修正前，既有法規未有規定者，由中央目的事業主管機關會商中央主管機關，依本法規定解釋、適用之。

七、落實風險管控

本法於第16、17、19條設有風險管理規範，說明如下：

（一）訂定風險規範：為促進人工智慧穩健及安全發展，本法明定數位發展部應參考國際標準或規範，推動與國際介接之人工智慧風險分類框架，並應協助各目的事業主管機關訂定以風險為基礎之管理規範。另為強化人工智慧之可驗證性及人為可控性，並提升其可信度，各目的事業主管機關應視人工智慧應用風險管理之需要，循前項風險分類框架，訂定以風險為基礎之管理規範，並應協助相關產業自行訂定產業指引及行為規範，而若有本法第5條第1項所列之情事者（指人工智

慧之應用，有侵害人民、破壞社會秩序、國家安全、生態環境、歧視、廣告不實、資訊誤導或造假等違法情事），應依法令限制或禁止之。

（二）建立問責制度：為確保人工智慧之安全性並保障人民權益，政府應就高風險人工智慧之應用，明確其責任歸屬及歸責條件，並建立其救濟、補償或保險機制，而為避免影響學術研究自由及產業前端研發，特此規定人工智慧之研發，於實際應用前，不適用前項規定，但其於實際環境測試，或運用研發成果提供產品、服務時，則不在此限。

（三）建構內控機制：為落實風險管理，政府使用人工智慧執行業務或提供服務，應進行風險評估，規劃風險因應措施，而政府應依使用人工智慧之業務性質，訂定使用規範或內控管理機制。

結語

從本文可知，《人工智慧基本法》主係參考各先進國家及綜整我國現行法規所制定，對政府而言，規劃推動人工智慧發展政策，有本法揭櫫之七大原則及相關義務可供遵循；就企業而言，本法賦予人工智慧風險分類框架之法源依據，有助相關產業釐清界線，俾以訂定研發方向及行為規範，且可享有政府鼓勵發展所提供之資源；於民眾而言，本法則明確規範保障人民之相關權益，足見立意良好且確有必要。由於本法攸關政府、企業及民眾三方之權利義務，影響深遠不容小覷，尤其當前政府積極導入AI協助處理業務的同時，公務員亦應依法推行，如檢討修正法令、進行風險評估、建構內控機制等均屬要務，綜上可知，熟悉新法實為根本之道，此即撰寫本文宣導之初衷。