

人工智慧基本法

中華民國 115 年 1 月 14 日

華總一義字第 11500001671 號

第一條 為建設智慧國家，促進以人為本之人工智慧研發與人工智慧產業發展，建構人工智慧安全應用環境，落實數位平權，保障人民基本權利，增進社會福祉，提升國人生活品質，促進社會國家之永續發展，維護國家文化價值及提升國際競爭力，並確保技術應用符合社會倫理，特制定本法；本法未規定者，適用其他法律之規定。

第二條 本法所稱主管機關：在中央為國家科學及技術委員會；在地方為直轄市、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。

第三條 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。

第四條 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，進而提升人工智慧可信任度。

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。

第五條 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。

數位發展部及其他相關機關應提供或建議評估驗證之工具或方法，以利各目的事業主管機關辦理前項事項。

前項驗證工具及方式之形成，應徵詢相關利益團體、產業、學者、社會團體及法律專家之意見。

第六條 行政院應成立國家人工智慧戰略特別委員會，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。

前項委員會每年至少召開會議一次，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。

第一項委員會之幕僚作業，由國家科學及技術委員會辦理。

- 第七條 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。
- 第八條 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。
- 第九條 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。
- 第十條 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。
- 第十一條 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，在符合本法第四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。
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。
- 第十二條 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。
- 第十三條 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。
政府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。
- 第十四條 各目的事業主管機關會商個人資料保護主管機關，在人工智慧研發及

應用過程，避免不必要之個人資料蒐集、處理或利用，並應促進個人資料保護納入預設及設計相關措施或機制，以維護當事人權益。

第十五條 政府應積極運用人工智慧確保勞動者之勞動權益。

政府應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。

政府應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。

第十六條 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。

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。有第五條第一項所列之情事者，應依法令限制或禁止之。

第十七條 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。

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，不在此限。

第十八條 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，應自本法施行後二年內，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。

第十九條 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。

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。

第二十條 本法自公布之日起施行。