議案編號：202103235150000

立法院議案關係文書 （中華民國41年9月起編號）
中華民國112年12月6日印發

院總第 20 號　委員提案第 10043021 號

案由：本院台灣民眾黨黨團，鑑於人工智慧發展，將為我國下個戰略趨勢，並且人工智慧將廣泛運用於各種社會生活及經濟活動，而國際上針對人工智慧所可能發生之風險，如歐盟、加拿大等國均提出專法，針對人工智慧系統提出風險分級管理的模式。為使人工智慧管制能有效管理，避免人工智慧成為侵害人民基本權的系統，並以建立「可信賴之人工智慧」為基礎促進人工智慧之發展，爰擬具「人工智慧發展及管理條例草案」。是否有當？敬請公決。

說明：人工智慧在千禧年後，因電腦運算能力持續提升、資料儲存成本下降及半導體技術的進步與成本降低，人工智慧進入第三波發展階段，隨著近年來自駕車、生成式人工智慧的出現，人工智慧帶來更高的工作效率，並為促進人類生活開啟新的契機。然而科學家霍金曾言：「全面發展 AI 的話，人類恐自取滅亡」，即表達出 AI 帶來生活便利、行政效率的同時，對於人類可能帶來許多的危險，如資料之偏誤所帶來的就業性別歧視等，而面對新的 AI 科技發展，各國亦紛紛提出相關的監管規範，如歐盟、德國、英國、美國、OECD、G20，私人企業 Google、微軟等均有提出相關倫理準則，甚至制定專法，來回應新科技所帶來的柯林格里奇困境，以在科技發展的同時，適度防堵對於使用者或一般人民基本權之危害。

現行人工「智慧」何謂智慧之定義較有爭議，因此宜採取較為概括性的論述，將所有之風險納入管制。另外，為防堵對於可預期的基本權侵害，防患於未然，促進 AI 商品或服務之跨國流通性，適度解決歐盟的布魯賽爾效應帶來的問題，本法擬建構以人為本、值得人民信賴的 AI，以歐盟之「預防原則」作為本法的立法基礎，由於 AI 之風險均不相同，而應以風險為基礎進行人工智慧系統或商品之規制；另外設計足夠之可問責性機制以及相關文書提出義務，以事後的觀點來填補人工智慧系統科技發展下所帶來不便利性；最後，為兼及人工智慧之發展亦提出相關創新鼓勵之措施，來鼓勵人工智慧之發展，爰擬具「人工智慧發展及管理

條例草案」，其要點如下：

一、本法之立法目的、適用範圍。（第一條）

二、本法之中央主管機關為數位發展部；各地方則為縣市政府。（第二條）

三、本法之名詞定義。（第三條）

四、主管機關掌理之事項。（第四條）

五、政府應寬列預算，由國家發展基金投入人工智慧產業並提供財稅及金融優惠制度，以培植國內人工智慧人才促進人工智慧產業發展。（第五條至第七條）

六、政府應針對人工智慧產業發展及相關事項設置專職機構辦理。（第八條）

七、政府應創造通用格式之巨量資料分享平台，由政府推廣、確立資料有價之理念，並鼓勵私人將巨量資料投入巨量資料分享平台，以建構相當資料利於人工智慧之發展。（第九條、第十條）

八、人工智慧之發展原則應以人為本，並善盡環境永續及社會福祉，於發展中倘若涉及資料之處理及利用，亦應善盡個人資料自主之保障；為建構可信賴之人工智慧，應確保其避免歧視之特定以及善盡其可問責性並防止不公平競爭。（第十一條至第十六條）

九、人工智慧之使用、研發，涉及個人資料之蒐集、處理、利用及傳輸之行為，亦應善盡個人資料保護之規定，並對應 GDPR 賦予當事人資料可攜權。（第十七條）

十、人工智慧之發展，應以風險為分級，特別是高風險之內容，涉及較多法遵成本，應由諮詢評估會議議定之。（第十八條）

十一、高風險人工智慧其研發者及提供產品服務者應由其研發長向主管機關提交安全監測計畫、安全監測報告、建立風險管理系統，並向中央目的事業主管機關提出合乎法規規定之技術文件。（第十九條至第二十二條）

十二、主管機關針對高風險之人工智慧研發及利用，應設置監測體系，必要時得採取相關措施防止損害。（第二十三條）

十三、高風險人工智慧應確保其自動記錄功能，並於主管機關指定之網站公告相關資訊，確保人工智慧之透明性，以成為可信賴之人工智慧。（第二十四條、第二十五條）

十四、人工智慧於發生嚴重影響生命身體之事，其研發者或提供產品之人，應立即通報目的事業主管機關。（第二十六條）

十五、特殊人工智慧系統，因其具備詐欺之風險及特性，無論是否為高風險人工智慧，均有規範之必要，因此針對與自然人互動之人工智慧系統、情緒識別或生物識別之人工智慧系統，或人工智慧系統用於生成影音，而內容易被誤為真實者，明文規定揭露、資料蒐集等義務。（第二十七條至第二十九條）

十六、人工智慧創新實現場域之推動、核准及審查之程序。（第三十條、第三十一條）

十七、主管機關應推動之人工智慧發展事項。（第三十二條）

十八、人工智慧之民事責任、政府應建立社會保險制度及無法救濟時應請求人工智慧之國家救濟補償。（第三十三條至第三十五條）

十九、損害個人資料、違反風險管理系統、提出技術文件、安全監測計畫及報告、記錄功能、人工智慧系統資訊之揭露義務、未依個人資料提供通用格式之資料或其內容有虛偽不實或違反本法之通知義務之處罰。（第三十六條至第三十九條）

二十、政府之法令檢查及完備義務（第四十條）

二十一、本法之施行日期。（第四十一條）

提案人：台灣民眾黨立法院黨團

吳欣盈　陳琬惠　賴香伶

張其祿　邱臣遠

人工智慧發展及管理條例草案

條　　文	說　　明
第一章　總　　則	章名。
第一條　為促進我國人工智慧技術及人工智慧產業之發展，建立安全及可信賴之人工智慧環境，提升國民生活福祉及國家競爭力，維護人類社會之永續發展，特制定本法；本法未規定者，適用其他法律之規定。 軍事用途所發展之人工智慧技術，不適用本法之規定。	一、本法之立法目的。 二、我國近年來於人工智慧相關領域發展進步迅速，而人工智慧發展為一新興領域，涉及複雜之管理，亟需要完善之法制基礎，建構相關發展體制。考量歐盟、日本、美國等先進國家多訂立有相關專法，組設專責機構推動人工智慧發展，我國亦成立數位發展部，正式將人工智慧列入其數位產業署之職掌範圍，自應及早進行相關法制規範，爰制定本法。 三、為確立本法之基本法地位，並調和與其他法規範間之適用關係，爰於本條後段規定，於本法未規定時，其他法律有規定者，應優先適用其他法律之規定。 四、基於軍事用途之人工智慧技術發展，有其特別考量，倘若均須依本法採取對應之措施，有妨礙國家安全之虞，爰於第二項明文排除之，並由國防部另訂相關規則以辦理軍事人工智慧之發展。
第二條　本法之主管機關為數位發展部；在地方為直轄市、縣（市）政府。 本法所定事項，涉及各中央目的事業主管機關職掌者，由各該機關辦理。	一、數位發展部於 111 年設立，職在推動數位經發展，建設國家數位轉型之任務。且參酌數位發展部組織法第二條之規定，數位發展部掌理國家數位發政策之擘劃，均與人工智慧之發展息息相關，爰明列本法之主管機關為數位發展部；人工智慧之發展，應不區分中央及地方，地方縣市政府之各局處均有導入人工智慧辦理相關業務之可能性，因此地方政府亦有主管相關業務之必要。 二、又人工智慧所涉之事項多元，有賴於各部會之間相互配合以及調和，尚包含國家發展基金之挹注、政府資料公開、個人資料運用、智慧財產保障、人工智慧產業發展、人工智慧之跨領域應用及法規制（訂）定、修正或廢止等不同中央目的事業主管職掌之業務等，爰為第二項規定。

第三條　本法用詞，定義如下： 一、人工智慧：指接收人類或機器資料輸入，以下列各目全部或部分方式，實現預測、建議、決策或其他特定目的之軟體、硬體及其他相關之系統： (一)使用監督式學習、非監督式學習、強化學習或其他利用資料建立模型之機器學習之方式。 (二)使用各種知識表示方式之知識庫系統，以推理引擎進行歸納、演繹、反正或其他模仿人類邏輯推理能力之方式。 (三)利用統計、搜尋、剖析、優化或其他方法，建立決策或推理模型之方式。 (四)使用前三款以外之模仿人類思考及反應模式，進行感知、規劃、推理、學習、溝通、修正或其他之方式。 二、人工智慧產業：指包含政府、法人單位、學術機構及民間廠商對於人工智慧研究、人工智慧技術關鍵基礎設施之研發、設計、製造、修護、組裝及檢驗、人工智慧應用服務（含營運）及其衍生之新型態服務產業等領域。 三、巨量資料：指規模巨大，且無從直接或間接識別特定個人之數據資料，並可藉由資料蒐集、數據儲存、資訊萃取、統計分析達到決策建議，創造創新價值。 四、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、種族、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動、政治意見、宗教信仰及其他得以直接或間接方式識別該個人之原始資料。 五、人工智慧安全：指防止人工智慧應用之相關資料、系統及裝置遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其準確性、完整性及可信賴性。	一、本法用詞之定義。 二、第一款所定人工智慧之定義，係指使用可以體現或模仿人類行為及反應之方式，作為預測、建議或決策等特定目的之軟體、硬體或其他開發中之系統，針對尚在發展中之技術定義上顯有困難，爰參考財團法人人工智慧法律國際研究基金會為第一項之名詞定義。 三、第二款所定人工智慧產業定義，係參酌現行「太空發展法」第三條條文內容，就類似型態之新興領域產業予以修正。 四、第三款所稱巨量資料，亦稱為「大數據」（big data）；其定義係參酌現行依「產業創新條例」訂定之「公司或有限合夥事業投資智慧機械與第五代行動通訊系統及資通安全產品或服務抵減辦法」第二條所示，又考量人工智慧領域之巨量資料，應以非屬個人資料之結構或非結構數據使用於機器學習或演算法等資料訓練過程，爰另與個人資料性質明確予以區分。 五、第四款所定個人資料定義，係參酌現行「個人資料保護法」第二條定之，另參酌歐盟「一般資料保護規則」（General Data Protection Regulation, GDPR）列舉之特殊具敏感性之個人資料範疇，將種族、政治意見及宗教信仰列入個人資料定義範圍。 六、第五款所稱人工智慧安全，係指第一款所列之人工智慧任一相關技術及其物聯網中任一連接裝置，遭受未經授權之侵害，導致不可預知之決策結果（例如自駕車判別錯誤導致意外發生等），其與一般所稱之資通安全應有所區別，爰予以明定。
第四條　主管機關掌理下列事項： 一、國家人工智慧發展基本政策之擬定。	一、第一項明定主管機關掌理事項。 二、為執行通用格式之巨量資料平臺、訂定人

二、國家人工智慧計畫之規劃、訂定及宣導。 三、人工智慧產業之發展。 四、人工智慧創新實驗環境之推動、辦理、管理及督導。 五、通用格式之巨量資料平臺之統籌、協調、建置及督導。 六、人工智慧及人工智慧安全相關軟硬體技術規範、服務及審驗機制之訂定。 七、人工智慧發展相關倫理審查機制之訂定。 八、國際交流合作計畫之訂定。 九、國際人工智慧法制之研究。 十、其他有關人工智慧發展之統籌協調事項。 前項第五款至第九款事項，主管機關得委託法人、團體或機構辦理。	工智慧相關審驗機制、訂定倫理審查機制及訂定人工智慧相關國際合作交流計畫，並考量此類事項之專業性及技術性，爰於第二項明定主管機關得委託法人、團體或機構，協助辦理第一項第五款至第九款之事項，以符實際需要。
第五條　政府應於國家財政能力範圍內，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。	一、參考財團法人人工智慧法律國際研究基金會草案第六條文字。 二、為確保政府發展人工智慧產業能有充足之資源，以達到本法第一條所稱提升國民生活福祉與保障國家競爭力，自有必要確保其所需經費無虞，爰參考中醫發展法第四條及文化創意產業發展法第八條之規定，明定政府應寬列經費，確保落實人工智慧政策之經費穩定充足發展。
第六條　中央政府應積極協助、輔導人工智慧產業，結合財稅及金融優惠制度，提供產業穩健發展，培植國內人工智慧人才及產業鏈，促成人工智慧及經濟發展。	一、參考財團法人人工智慧法律國際研究基金會草案第七條文字。 二、政府應積極投入資源發展人工智慧，促成人工智慧產業發展經濟規模，鞏固我國在數位科技產業鏈之全球地位，故參考海洋基本法第九條規定，於本條規定政府應建構健全之產業環境，持續培育人才完備人工智慧產業鏈。 三、所稱財稅及金融優惠制度，係指所設中央目的事業主管機關依第五條第二項辦理之具體人工智慧發展相關措施。為保留其廣泛適用性，於本法揭示原則性、綱要性之精神。
第七條　國家發展基金應提撥一定比例投資人工智慧產業。	一、為揭示政府對於人工智慧領域之主導立場，爰於第一項明定人工智慧產業資金來

前項投資之審核、撥款機制與績效指標等相關事項之辦法，由中央主管機關會同相關目的事業主管機關定之。	源。 二、考量國家發展基金涉及不同目的事業主管機關之決策，爰為第二項規定。
第八條　為執行國家人工智慧基本政策及計畫，協助推動人工智慧技術及人工智慧產業發展相關事項，政府應以專責機構辦理相關業務。	考量世界各先進國家多設有專責機構或跨部會性質之專責委員會，為順利推動我國人工智慧發展相關事項，爰明定政府應以專責機構辦理相關業務。
第九條　主管機關應定期彙集人工智慧其研發者，或提供產品、服務之自然人、法人、機關、機構或團體依其職權取得或作成，且依法得公開之文字、數據、圖片、影像、聲音、詮釋資料及其他類型電子資料，以非屬個人資料之數據形式，建立通用格式之巨量資料平臺分享機制。 前項巨量資料平臺之資料彙集、去識別化或分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之。	一、為促進政府資料公開之實際效益，並創造人工智慧產業發展空間，提供未具一定規模之新創產業投入人工智慧領域之發展空間，應建立通用格式之巨量資料共享機制，爰為第一項規定。 二、第二項明定巨量資料平臺設置相關事項之辦法，由主管機關定之，以資遵循。
第十條　主管機關應推廣巨量資料有價之觀念，充分開發、運用非屬個人資料之數據資產，並落實於相關政策。 政府用於有形或無形之人工智慧相關資產支出，經濟效用年限達二年以上者，應劃編為資本門經費預算。 各中央目的事業主管機關應訂定各項獎勵或輔導措施，以鼓勵公民營企業及人工智慧產業，將巨量資料資產投入前條之巨量資料平臺，使人工智慧技術研發及創新成果，轉化為實際之生產或運用。	一、人工智慧技術之展現，高度取決於資料之品質、正確性及一致性，藉以避免資料訓練過程逐漸導致偏差而對人類世界有負面影響，顯見巨量資料足以成為人工智慧領域之關鍵資產，亦為其資料彙集之專業技術成果，爰於第一項明定巨量資料具備之智慧財產特性，主管機關亦應會同相關中央目的事業主管機關評估現行著作權法等相關法規修正之必要。 二、第二項明定人工智慧相關資產支出在一定時間後可劃編為資本門之規定，以突顯人工智慧有形、無形之價值。 三、為建立巨量資料或其演算技術為智慧財產概念，並鼓勵產業將巨量資料資產投入前條所定通用格式之巨量資料平臺意願，爰於第三項明定政府應訂定相關獎勵或輔導措施。
第二章　人工智慧發展之基本原則	章名。
第十一條　人工智慧發展應尊重國際公約及相關規範，以維護人性尊嚴及免於遭受生命、身體、自由、財產等法益之危害。	從事人工智慧發展必須尊重國際公約及相關規範，並參考歐盟之「可信賴的人工智慧綱領」（Ethics Guidelines for Trustworthy AI）中以強調維護人類主體性之原則，並避免基本權之侵害，落實「以人為本」之人工智慧發展精神，爰為本條規定。

第十二條　人工智慧發展應以環境保護、永續發展以及社會福祉為原則，確保環境安全，減少對環境之不利影響以及提升人民生活品質。	為因應聯合國永續發展目標（Sustainable Development Goals, SDGs），並善盡歐盟「可信賴的人工智慧綱領」（Ethics Guidelines for Trustworthy AI）中保護社會與環境利益之精神，從事人工智慧發展，應依國內各項環保法規及採取社會福祉之原則，爰為本條規定。
第十三條　人工智慧之發展所涉相關個資及資料庫、資料平台之建構，應善盡隱私及資料自主之保障，並確保資料之品質以維護人工智慧系統之可靠性。	人工智慧發展不免會侵害到個人隱私，為免個人隱私及資料自主遭到破壞，並為避免資料品質影響人工智慧之可靠性，並參考歐盟之「可信賴的人工智慧綱領」（Ethics Guidelines for Trustworthy AI）及美國之「人工智慧應用管制指引」（Guidance for Regulation of Artificial Intelligence Application）中保障隱私及為資料治理之原則，爰明文規範人工智慧之資料保障義務及資料治理責任。
第十四條　人工智慧發展在符合國家安全、人民權益及產業利益原則下，應公開相關資訊，並應強化人工智慧之可解釋性、透明性及可追溯性，並確保其問責之可能性。	人工智慧發展涉及智慧財產及商業利益，同時亦與民生安全及社會秩序有關，爰參考歐盟之「可信賴的人工智慧綱領」（Ethics Guidelines for Trustworthy AI）及美國之「人工智慧應用管制指引」（Guidance for Regulation of Artificial Intelligence Application）明定人工智慧發展應秉持透明為原則，以促進國民了解人工智慧之運作機制，促進人工智慧之使用普及性。
第十五條　人工智慧之研發及利用，應促進多元並避免產生對特定族群之偏見。 政府於應用人工智慧應優先考量身心障礙者、高齡者、兒童及其他需要協助族群之權益；必要時應賦予利害關係人之參與機制。	一、人工智慧之應用可能產生歧視與偏見的問題，且歐盟之「可信賴的人工智慧綱領」（Ethics Guidelines for Trustworthy AI）以及美國之「人工智慧應用管制指引」（Guidance for Regulation of Artificial Intelligence Application）中基於上述考量，亦強調此倫理要件，爰明文規定於第一項。 二、又政府利用人工智慧應在謀求全民福祉及保障所有人對於人工智慧之可近用性，爰參考財團法人人工智慧法律國際研究基金會草案第十條規定於第二項明定人工智慧之優先考量及參與機制。
第十六條　政府應防止人工智慧之研發或利用者，以其優勢地位為資料之不當蒐集、處理、利用或從事不公平競爭，確保交易秩序及消費者權益。	一、參考財團法人人工智慧法律國際研究基金會草案第十二條文字。 二、政府為確保交易秩序及消費者權益，應防止人工智慧之研發或利用者，以其優勢地位進行不當資料蒐集或實施不公平競爭。

第三章　人工智慧之管制及風險管理	章名。
第十七條　人工智慧之研發及利用，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體進行人工智慧技術研發或應用時，若涉及個人資料之蒐集、處理、利用及傳輸等行為，應以取得當事人同意、履行契約或其他法令授權者為限，並適用個人資料保護法第三條規定。 前項之利用個人資料者，應以適當之去識別化方式，將個人資料轉化為無從直接或間接識別特定個人之數據資料。 當事人得要求第一項之利用個人資料者以通用格式提供其個人資料。	一、為確保人民基本隱私權不受人工智慧技術侵害，爰於第一項明定不同身分之人工智慧開發者皆應遵守個人資料保護法對於當事人權益之保障。 二、鑒於將個人資料經去識別化措施而產生之結構或非結構式數據，不僅為對個人資料當事人隱私權益保障之義務，亦為巨量資料彙集之基本要求，爰於第二項明定不同身分之人工智慧技術開發者應將個人資料轉化為非屬個人資料之數據形式。 三、考量個人資料當事人同意參與人工智慧技術應用過程中，仍應隨時保有其個人資料之可攜性，且得要求以通用格式進行移轉，爰為第三項規定。
第十八條　主管機關應採行之人工智慧管理措施應以風險評估為基礎，符合滿足國民接近使用人工智慧、確保安全之人工智慧、事先預防原則、資訊透明原則，建構風險分級責任制度。 前項之風險分級責任制度由高至低，分為不可接受風險之人工智慧、高風險之人工智慧、特定風險之人工智慧及風險極小之人工智慧。 第二項高風險之人工智慧之內容，應由主管機關召集人工智慧、風險管理、法律或相關領域之專家學者及所評估產業之產業代表，組成風險評估諮詢會議並參考國際標準、以及產業競爭力以個別產業逐案表決、討論之方式定之。其組成成員之單一性別及產業代表不得少於三分之一。 第三項之會議之審議表決辦法，由中央主管機關定之。	一、考量人工智慧系統之發展，可能伴隨隱私外洩、歧視等對使用者或使用對象造成嚴重基本權侵害之情形，因此參酌歐盟「人工智慧法案」（Artificial Intelligence Act），為平衡人工智慧新科技所帶來之風險，及避免過度限制或阻礙新技術之發展，應依「預防原則」建立風險評估及監管機制，依風險特定及高低程度，進行適當管制。 二、第二項參酌歐盟「人工智慧法案」（Artificial Intelligence Act）之規定，將風險區分為不可風險之人工智慧、高風險之人工智慧、低風險之人工智慧及風險極小之人工智慧。 三、鑑於人工智慧高度不可控制性及不確定性之特性，並隨著人工智慧系統之技術提升、應用成熟，其所潛在之問題或風險亦會顯現與明朗，故其風險事由有隨時調整之必要，故其原則上宜由主管機關會同專家學者，針對人工智慧系統可能造成之風險，進行風險分級。 四、為避免斲喪產業競爭力，在評估前針對是否列入為高風險人工智慧之分級內容，除應考量其產業風險外，亦應考量相關產業競爭力，故應由產業代表列席，並藉由人數限制，賦予其陳述意見及表決之機會。

第十九條　高風險人工智慧之研發及利用，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體，應向各目的事業主管機關提出安全監測計畫，並經核定後，始得為之。	一、參考自參考財團法人人工智慧法律國際研究基金會草案第十七條文字。 二、為確保人工智慧研發及利用之安全性，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體、應向各目的事業主管機關提出安全監測計畫。衡酌人工智慧之運用，相關風險之控管，中央目的事業主管機關協力應要求上開人員提供安全監測計畫，其安全監測計畫內容，由中央目的事業主管機關核定。
第二十條　人工智慧之研發及利用，經評估為高風險者，其研發者，或提供產品服務之自然人、法人、機關、機構或團體，應依主管機關之規定，建立風險管理系統，以識別、評估該系統可能造成的損害或有發生偏見之風險，並制定風險防範之措施。 高風險人工智慧系統，依其風險管理系統之評估，有重大變更，其研發者，或提供產品服務之自然人、法人、機關、機構或團體，應立即通知主管機關。	一、為確保人工智慧之安全性，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體，基於預防原則之考量，參考歐盟「人工智慧法案」（Artificial Intelligence Act）第九條以及加拿大人工智慧與數據法草案（The Artificial Intelligence and Data Act）第八條，應建立起風險管理系統識別，用以識別、評估該系統可能造成的損害，並針對其所發生之損害風險或偏見風險，提出防範之措施。本條所稱之風險防範措施，除其他防範措施外，更應包含歐盟「人工智慧法案」第 14 條確保人工智慧系統生命週期內人為之有效監督機制。 二、倘若隨情事變更，而致風險有所變化，無論是主觀危險增加亦或客觀危險增加，均應立刻通知主管機關，俾利主管機關得隨時掌握風險，避免人工智慧系統所導致之損害擴大。
第二十一條　人工智慧於上市或提供服務前，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體，應向中央目的事業主管機關提出符合法規規定之技術文件，並予公開。	一、為確保人工智慧之安全性，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體，應向中央各目的事業主管機關提出符合法規規定之技術文件。為能讓政府適當監管，爰參考歐盟「人工智慧法案」（Artificial Intelligence Act）第 11 條、財團法人人工智慧法律國際研究基金會草案第十七條文字，相關技術文件應有必要提供予中央目的事業主管機關知悉。 二、另，基於人工智慧之透明性及可解釋性之確保，相關技術文件應予公開，惟涉及營業秘密或專利技術之內容，依相關法令之規定，自當不予公開。

第二十二條　高風險人工智慧於上市或提供服務後，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體，應定期向目的事業主管機關提出安全監測報告，以利監測其風險變化及確保防範措施之有效性。	一、為因應人工智慧應用之風險及變動性，確保其上市或提供服務後仍符合本法相關規定以及確保安全無虞，主管機關應有必要適時掌握人工智慧之研發、產品與服務之風險及安全。 二、據此，人工智慧之研發者，或提供產品、服務之自然人、法人、機關、機構或團體，應有定期向目的事業主管機關提出安全監測之報告，爰參考財團法人人工智慧法律國際研究基金會草案第十八條文字，增訂安全監測報告之提出義務，以利目的事業主管機關得確實掌握人工智慧於上市或提供服務後，能持續監管其潛在之風險。
第二十三條　各級主管機關對高風險之人工智慧之研發及利用，建立高風險人工智慧監測體系，於下列情形時，應主動查驗，並發布預警或採行必要之管制措施： 一、高風險人工智慧系統安全性有欠缺。 二、高風險人工智慧系統準確性、穩健性有欠缺。 三、高風險人工智慧系統之可解釋性有欠缺。 前項主動查驗、發布預警或採行必要之措施，由中央主管機關定之。 第一項各款監測內容之基準，應由中央主管機關會同各目的事業主管機關考量各產業之性質並參考國際標準具體公告之。	一、人工智慧之風險管控機制，除有賴於人工智慧系統之研發者及利用者之自律行為外，亦應仰賴主管機關「他律」之監督模式，以確保人工智慧之安全性、準確性以及穩健性，基於相同風險控管之考量，爰參考食品安全衛生管理法第五條、歐盟「人工智慧法案」（Artificial Intelligence Act）第十五條規定，主管機關應建立起人工智慧監測體系，於監測發現有安全性、準確性、穩健性以及可解釋性欠缺，以致人工智慧系統有損害或追溯困難之風險時，應發布相關措施，以降低損害風險。 二、至第一項所稱之「安全性」、「準確性」、「穩健性」、「可解釋性」等標準，應參酌前開風險預防機制等技術性、細節性事項隨人工智慧變遷，亦有調整之必要，故授權主管機關訂定並公告之，使相關企業知悉，並降低法遵成本。
第二十四條　高風險之人工智慧之研發及利用，其研發者應設計和開發符合主管機關標準之人工智慧系統執行時之自動記錄功能，以確保高風險人工智慧系統之可追溯性及可問責性。 高風險人工智能系統，其記錄功能應包含下列事項： 一、記錄系統每次使用的時間段。 二、系統對輸入數據進行檢查的參考數據庫。 三、導致搜索結果之輸入數據。	一、為使人工智慧系統之可問責性得以被確保，又衡酌人工智慧系統因其運算過程未必全然詳盡且透明，而對舉證產品研發、開發者具過失、因果關係等待證事實顯有困難，因此參酌歐盟「人工智慧法案」（Artificial Intelligence Act）第十二條及加拿大「人工智慧和數據法案草案」（Artificial Intelligence and Data Act）第十條規定，明文規定，應建立執行時之自動記錄功能。 二、此項規定，非僅有實體法上之建置保存義

四、其他主管機關所定事項。	務，於訴訟法上，亦有證明妨礙之制度可加以援用，以減輕當事人在可問責性上之舉證負擔。
第二十五條　高風險人工智慧之研發及利用，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體之應以清晰易於理解之方式，在主管機關指定之網站公告下列資訊，以確保人工智慧系統之可近用性及透明性： 一、人工智慧系統之使用方式。 二、系統所欲達到之預期目的及效果。 三、資料蒐集籍資料品質驗證之策略、程序、措施及工具。 四、對使用者造成之風險及風險防範措施。 五、其他主管機關所定事項。	考量人工智慧系統之可追溯性及透明性為人工智慧產業之基本義務，以健全人工智慧之可問責性，爰參酌歐盟「人工智慧法案」（Artificial Intelligence Act）第十三條及加拿大「人工智慧和數據法案草案」（Artificial Intelligence and Data Act）第十一條規定，明定人工智慧之研發、利用者之資訊揭露義務，以確保人工智慧系統之使用者，能安心使用人工智慧系統，以促進本法第一條之可信賴人工智慧環境。
第二十六條　人工智慧於研發、上市或提供產品、服務後，發生嚴重影響人民生命、身體、自由或財產之情事，其研發者或提供產品、服務之自然人、法人、機關、機構或團體，應立即通報目的事業主管機關。	一、參考財團法人人工智慧法律國際研究基金會草案第十九條文字。 二、為控制人工智慧之風險，人工智慧於研發中、上市或提供產品、服務後，發生嚴重影響人民生命、身體、自由或財產之情事時，參考食品衛生安全管理法第七條第五項，食品業者於發現產品衛生安全之虞時，應通報直轄市、縣（市）主管機關之規定，如人工智慧之利用發生上述情形，其研發者或提供產品、服務之自然人、法人、機關、機構或團體，亦負擔即時通報義務。
第二十七條　以與自然人互動為設計目的之人工智慧系統，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體應使互動自然人知悉其與人工智慧系統互動。但與其互動之自然人明顯可知其係與人工智慧系統或於經法律許可之刑事偵訴人工智慧系統不在此限。	一、以與自然人互動之人工智慧系統，不論是否為高風險人工智慧系統，縱使其可能造成之損害較小，但因其仍帶有遭欺騙之特別風險，因此有透明化之必要，爰參考歐盟「人工智慧法案」（Artificial Intelligence Act）第五十二條第一項規定，增訂其與人工智慧系統互動之告知義務。 二、例外於與其互動之自然人明顯可知之情況下，應不至於發生誤認人工智慧之情形，無加以規範之必要，如：掃地機器人，則無需加以告知；或基於犯罪預防與偵查之目的，為避免告知義務妨礙其偵查目的之達成，宜例外設排除規定。
第二十八條　情緒識別或生物識別之人工智慧	一、使用情緒辨識或生物特徵分類有涉及個人

系統，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體應告知接觸該系統之自然人之執行情況。但經法律許可之刑事偵訴生物識別系統，不在此限。	高度敏感性資訊，其使用人工智慧系統亦有透明化之必要，即應告知受辨識者正在接受情緒辨識功能，爰參考歐盟「人工智慧法案」（Artificial Intelligence Act）第五十二條第二項規定，增訂其與情緒辨識或生物特徵分類之告知義務。例外亦在經法律規定許可之犯罪預防、追溯目的時，得免除告知義務。 二、另本條雖容許刑事偵查機關基於刑事目的為情緒辨識或生物特徵之追溯，然此處僅是免除告知義務，並非在授予偵查機關為此項科技偵查、強制處分之法律基礎，立法者仍應以科技偵查法或刑事訴訟法定之，併予說明。
第二十九條　人工智慧系統用於生成或操縱影像、音訊、影片等內容，其內容近似於現存在之人、物、地點或其他實體事件，且依一般社會觀念易被認為真實者，其研發者，或提供產品、服務之自然人、法人、機關、機構或團體應揭露其內容為人為生成、製造。	使用人工智慧系統生成影像、音訊、影片等涉及深偽（Deep Fake）技術內容，而有使人陷於偽造、變造確為真實。AI 使用者必須揭露其內容係經人工製造，使資訊接受者知道內容非真實，以避免詐欺風險。
第四章　人工智慧之推動及創新實驗領域	章名。
第三十條　主管機關為推動人工智慧技術創新，應協助辦理人工智慧產業之創新實驗申請許可、核准或特許。 前項創新實驗申請，應經倫理審查委員會（以下簡稱審查會）審查通過，始得為之。 前項審查，主管機關得委託第六條之專責機構設立審查會為之。 創新實驗內容之變更，應以未涉及該實驗之重要事項，且對參與者之權益無重大影響者為限；其變更應經原審查通過之審查會同意後，始得實施。 前四項創新實驗申請或變更之審查、評估、許可、核准或特許等條件及程序等相關事項之辦法，由主管機關會商中央目的事業主管機關定之。	一、為加速人工智慧創新、協助規模較小之新創公司投入人工智慧發展之可及性、實用性及品質，爰參考國際盛行之監理沙盒（sandbox）制度，於第一項明定在不影響社會秩序及消費者權益下，對於辦理人工智慧技術創新，可能有牴觸法規之虞，或因測試之需要而有排除適用相關法規之必要，或業務範圍依法規難以判斷為適法者，許其得提出創新實驗之申請。 二、鑒於創新實驗包括跨領域之應用，為確保審查機制之妥善，並兼顧相關領域之意見，明定創新實驗計畫應送交倫理審查委員會審查。 三、為兼顧創新實驗之穩定、參與實驗者及其隱私權益之保護，爰於第三項明定實驗內容之變更僅限於有必要性且顯無重大權益影響之情形，且須再經倫理審查委員會審查同意。 四、第四項明定創新實驗申請或變更之相關辦

	法，授權由主管機關會商中央目的事業主管機關定之，我國於無人載具條例，亦設有相關創新實驗之規範，可供參照。
第三十一條　審查會應獨立審查。 主管機關依第六條設立之專責機構應確保審查會之審查不受主管機關或專責機構之不當影響。	一、為確保審查會必須獨立於申請者、贊助者、或任何其他不當影響力之外，爰為第一項規定。 二、前項所稱獨立審查原則，亦包含主管機關或專責機構本身之不當影響力，爰另於第二項明定研究機構之義務，以確保獨立審查之落實。
第三十二條　為促進我國人工智慧產業之健全發展，主管機關應會同各中央目的事業主管機關，推動下列事項： 一、鼓勵民間投資人工智慧事業。 二、推動高附加價值之人工智慧技術產業應用及必要之獎勵措施。 三、協助關聯產業發展及國際接軌。 四、培育人工智慧產業發展人才。 五、輔導育成人工智慧新創事業。 六、促進涉及重大公共利益之跨領域人工智慧技術應用。 七、有關結合在地資源及人才，發展地方產業鏈，營造在地產業生活圈，及其他促進人工智慧產業發展之事項。	鑒於人工智慧產業之健全發展，亟需政府扶植與民間投入參與，相關具體事項包含民間投資、推動高附加價值之人工智慧技術產業應用及必要之獎勵措施、協助與國際接軌、人才培育、新創事業輔導等，爰明定主管機關應推動之相關事項。
第五章　人工智慧之問責機制	章名。
第三十三條　人工智慧系統商品之商品製造人，其所提供之人工智慧系統之服務或所製造之人工智慧商品因其商品之生產、製造或加工、設計欠缺所致他人之損害，對他人負賠償責任。 受害人已證明商品之生產、製造或加工、設計有欠缺者，推定商品製造人有過失。 就高度風險人工智慧商品，有如下情形之一者，推定該產品有瑕疵： 一、被告拒絕交付法院所要求之文書、準文書或勘驗物。 二、原告已主張並證明該產品不符合國家安全性之強制性要求，而此等要求乃在於避免該以產生損害之危險。 三、原告已主張與證明該損害乃透過該產品一項明顯錯誤功能，於通常情況下所	一、人工智慧系統為對人民隱私及其他基本權造成高度損害風險之危險活動，又基於促進社會發展考量，但考量其研發者、使用者自危險活動中大量獲利且根據其不可控制性以及事證偏在、武器不平等之情形，更是對其使用之對象造成舉證上之困難，因此基於風險分配上之正義，爰參考民法第一百九十一條之一之商品責任與德國產品責任法之規範，宜採取推定過失立法模式、推定因果關係之立法模式，以作風險之合理分配。 二、又人工智慧法制，賦予針對高風險人工智慧系統，採取長期之安全性保障，與消保法所規定流通入市場時符合當時科技或水準之「可期待安全性」不同，自應有不同之考量，且基於人工智慧之不確定性，對

產生。 前項產品，依具體事件之狀況，法院認為較有可能有瑕疵存在，則推定該產品有瑕疵。	企業而言未必舉證容易，自應排除消保法無過失責任之適用，俾利相關人工智慧不致因防衛性概念而阻礙人工智慧發展，而應採取本法之推定過失責任。 三、比較法上參酌歐盟人工智慧責任指令草案，第 3 條設有資訊提供請求權，其包含舉證困難時請求法院裁定提供資訊之義務以及本法所規範之資訊提供請求權，依此商品之消費者可以藉此向產品製造人或系統提供商請求相關之資訊。 四、另外，在本法亦設有相關商品瑕疵的規範，設計舉證減輕之相關規範，並在若干情形應推定該商品有瑕疵，並一同推定過失。
第三十四條　政府應審酌人工智慧研發及利用所生之風險，建立必要之社會保險制度及人工智慧之問責方式。	一、有鑒於人工智慧發展迅速，未來成為大眾日常生活之一部分亦未可知，基於預防原則的考量，人工智慧相當程度之風險，政府應參考強制汽車責任保險等社會保險，建立起人工智慧之社會保險制度，以分散風險，促進人工智慧之發展與建立可信賴之人工智慧。 二、然此章之相關責任規範，怕本法無法全面且周全的解決相關責任問題，因此仍保留相當空間，在未來倘若有需要亦不排除制定相關人工智慧責任或（及）補償專法。
第三十五條　政府因發展人工智慧而導致人民受生命、身體之損害者，人民得請求向國家救濟補償。 前項請求權，自請求權人知有受害情事日起，因二年間不行使而消滅；自受害發生日起，逾五年者亦同。 中央主管機關於辦理人工智慧風險之核定時，徵收一定金額充作人工智慧系統受害之救濟基金。 前項徵收之金額、繳交期限、免徵範圍與預防接種受害救濟之資格、給付種類、金額、審議方式、程序及其他應遵行事項之辦法，由中央主管機關定之。	一、鑑於人工智慧運用層面廣泛，但因其不可控制性與不可預測性，即便窮盡相關監理措施或善盡善良管理人之注意義務，亦有可能對人民造成損害，於部分情形，尚難指摘為違法，而難以訴求國家賠償；此等情形亦非遭受特別犧牲，而得以請求損失補償。然國家發展人工智慧，卻無力全然排除人工智慧對人民生命、身體可能造成之損害，受害人之所以受損害與國家發展人工智慧間具有因果關係。為彌補此等漏洞，特別設計人工智慧之救濟，以善盡國家保護義務。 二、然參國內損失補償範圍多涉及生命、身體之案例，如：藥害救濟法，且為免人民動輒申請補償，擠壓其他申請人之資源，以促進資源有效利用，應限於生命、身體之

	損害，並參酌藥害救濟法之時效及其他相關規範增定其救濟制度。
第六章　罰　　則	章名。
第三十六條　違反第十七條第一項及第二項規定，足生嚴重損害於個人資料當事人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。	違反第二十一條第一項及第二項規定之處罰；其罰則係參酌「個人資料保護法」第四十一條等相似行為程度所定之刑度。
第三十七條　有下列各款情形之一者，主管機關應通知限期改正；屆期未改正者，處新臺幣二億元或企業年營收額百分之四以下罰鍰；情節重大者，並得命其歇業、停業一定期間、廢止其公司、商業、工廠之全部或部分登記事項： 一、未依第二十條之規定建立風險管理系統。 二、未依第十九條、第二十一條、二十二條規定，提出技術文件、安全監測計畫及安全監測報告。 三、違反第二十四條規定未依規定設計記錄之功能。 四、未依第二十五條公開揭露人工智慧系統之資訊。 五、違反第二十七條、第二十八條、第二十九條之通知義務者。 六、違反第二十一條第三項規定，妨礙、拒絕或規避提供個人資料當事人其通用格式之資料。	違反第十九條提供資料進行風險核定、第二十條風險管理系統建立義務、第二十一條技術文件並提供公開義務、第二十二條安全監測計畫或報告之製作義務、第二十四條記錄功能、第二十五條之資訊揭露義務規定之處罰；其罰則係參酌參考歐盟「人工智慧法案」（Artificial Intelligence Act）第 71 條行為程度所定之行政罰。
第三十八條　有下列各款情形之一者，主管機關應通知限期改正；屆期未改正者，處新臺幣一億元或企業年營收額百分之二以下罰鍰，並得按次處罰： 一、第十九條、第二十一條、第二十二條之技術文件、安全監測計畫及安全監測報告，其內容虛偽不實。 二、第二十四條之記錄內容，有偽造變造記錄之內容者。 三、第二十五條所揭露人工智慧系統資訊虛偽不實。	違反第十九條技術文件、第二十一條安全監測計畫、第二十二條之安全監測報告、第二十四條之記錄義務或第二十五條之揭露義務內容有虛偽不實之處罰；其罰則係參酌參考歐盟「人工智慧法案」（Artificial Intelligence Act）第 71 條行為程度所定之行政罰。
第三十九條　有下列行為之一者，處新臺幣一億元以下罰鍰或公司年營收額百分之一以下罰鍰；情節重大者，並得命其歇業、停業一	違反第二十條第二項及第十六條規定之處罰；其罰則係參酌食品安全衛生管理法第四十八條等相似行為程度所定之行政罰。

定期間、廢止其公司、商業、工廠之全部或部分登記事項： 一、違反第二十條第二項規定，未於風險變更時，通知主管機關。 二、違反第二十六條之規定，未於發生嚴重影響人民生命、身體、自由或財產之情事，立即通報主管機關。	
第七章　附　　則	章名。
第四十條　政府應依本法規定，檢討所主管之法規及行政措施；有妨礙人工智慧政策推定、不符合本法規定或無法規可資適用者，應自本法施行後三年內，完成法令之制（訂）定、修正或廢止，及行政措施之改進。 前項法規完成制（訂）定、修正前，由主管機關會商中央目的事業主管機關依本法規定解釋、適用。	一、為落實本法，確保人工智慧政策有效推動發展，政府應主動檢討相關法規及行政措施，是否符合人工智慧政策之推定，故參考海洋基本法第十六條規定，於第一項明定限期檢討法規。 二、依第一項規定應制（訂）定、修正前之相關法規，於未完成法定程序前，為使人工智慧相關事務能符合本法規定，參考海洋基本法第十六條第二項規定，於第二項明定中央主管機關會中央目的事業主管機關，依本法規定解釋、適用之。
第四十一條　本法施行日期，由行政院定之。	本條明定施行日期。