July, 2024

THY
Taiwan International
Law Offices

NEWSLETTER

台灣 AI 法制簡介

歐盟議會於 2024 年 3 月 13 日通過「人工智慧法案（Artificial Intelligence Act）」，成為全球首部針對人工智慧（Artificial Intelligence，下稱 AI）之法律規範。關於台灣 AI 相關現行之法制政策，簡介如下：

一、AI 核心價值與基本倫理

我國科技部（現為國家科學及技術委員會）於 2019 年 9 月提出「人工智慧科研發展指引（AI Technology R&D Guidelines）」（下稱本發展指引），期能完善 AI 科研環境與社會，引領台灣科研新局。

(一) AI 核心價值

本發展指引期待台灣能創建符合三大核心價值之 AI 社會：

1. 以人為本（Human-centered Values）：AI 發展應以提升人類生活並增進人類福祉為宗旨，構築符合人性尊嚴、自由與基本人權之人工智慧社會。
2. 永續發展（Sustainable Development）：AI 發展應追求經濟成長、社會進步與環境保護間之利益平衡，以人類、社會、環境間的共存共榮為目標。
3. 多元包容（Diversity and Inclusion）：AI 發展應以創建及包容多元價值觀與背景之 AI 社會為發展目標，並積極進行跨領域對話機制，提升民眾對 AI 之認識。

(二) AI 八大指引

此八大指引係衍生自三大核心價值，目的係抑制潛在疑慮與風險，消弭 AI 偏見、歧視與排除等情形，並促進人機合作。

1. 共榮共利（Common Good and Well being）
2. 公平性與非歧視性（Fairness and Non discrimination）
3. 自主權與控制權（Autonomy and Control）
4. 安全性（Safety）
5. 個人隱私與數據治理（Privacy and Data Governance）
6. 透明性與可追溯性（Transparency and Traceability）
7. 可解釋性（Explainability）
8. 問責與溝通（Accountability and Communication）

二、生成式 AI 參考指引

參考歐盟之定義，生成式 AI 模型係指一種電腦程式，旨在創建類似於人類製作（human-made）的新內容，其大量蒐集、學習與產出之資料，可能涉及智慧財產權、人權或業務機密之侵害，且其生成結果，因受限於所學習資料之品質與數量，而可能真偽難辨或創造不存在的資訊，須客觀且專業評估其產出資訊與風險。考量各行政機關利用生成式 AI 協助執行業務或提供服務，有助於提升行政效率，為促成各機關使用生成式 AI 有一致的認知與基本原則，並保持執行公務之機密性與專業性，我國行政院於 2023 年 8 月提出「行政院及所屬機關(構)使用生成式 AI 參考指引」（下稱本參考指引）。

本參考指引之規劃原則，簡介如下：

(一) **養成對生成式 AI 的正確觀念**：掌握自主權與控制權，並由業務承辦人客觀且專業評估生成式 AI 產出之資訊與風險。本參考指引強調，生成式 AI 產出之資訊，不得取代業務承辦人之自主思維、創造力及人際互動。

(二) **界定技術/工具運用的責任**：保持公務之機密性與專業性，並注意侵害智慧財產權與人格權之可能性。

(三) **建立必要的安全與內控機制**：各機關使用生成式 AI 作為執行業務或提供服務輔助工具時，應適當揭露，並遵守資通安全、個人資料保護、著作權等相關規定。各機關得依使用生成式 AI 之設備與業務性質，訂定使用生成式 AI 之規範或內控管理措施。

三、金融業運用 AI 之核心原則與政策

為協助金融機構善用 AI 科技優勢，並能有效管理風險、確保公平、保護消費者權益、維護系統安全及實現永續發展，金融監督管理委員會（下稱金管會）於 2023 年 10 月公布「金融業運用人工智慧(AI)之核心原則與相關推動政策」，揭示我國金融業運用 AI 之 6 項核心原則及 8 項配套政策，簡介如下：

(一) **建立治理及問責機制**：金融業使用 AI 應建立全面且有效的風險管理機制。

(二) **重視公平性及以人為本的價值觀**：金融業運用 AI 應儘可能避免演算法之偏見所造成的不公平，並符合以人為本及人類可控的原則。

(三) **保護隱私及客戶權益**：金融業以 AI 管理客戶資料時，須充分尊重及保護客戶的隱私權，並尊重客戶選擇是否使用 AI 服務的權利，提醒客戶是否有替代方案。

(四) **確保系統穩健性與安全性**：金融業應致力維護 AI 系統之穩健性及安全性，若運

用第三方業者之 AI 系統提供金融服務，則金融機構應對該第三方業者進行適當之風險管理及監督。

(五) **落實透明性與可解釋性**：金融業運用 AI 系統時，應確保其運作之透明性及可解釋性，並應於使用 AI 與消費者直接互動時適當揭露。

(六) **促進永續發展**：金融業應確保其 AI 發展策略及執行，符合永續發展相關原則，並盡力維護員工工作權益。

我國金融業運用 AI 之 8 項配套政策，簡介如下：

(一) **訂定「金融業運用 AI 指引」**：金管會於 2023 年 12 月底提出「金融業運用 AI 指引」草案，分為總則與 6 大章節，總則主要說明 AI 相關定義、AI 系統生命週期、風險評估框架、以風險為基礎落實核心原則的方式、第三方業者的監督管理等共通事項；6 大章節則分別說明金融業在落實 6 項核心原則時，依 AI 生命週期及所評估的風險，宜關注的重點以及可採行的措施，包括目的、主要概念，以及各原則相應的注意事項、落實方式或採行措施等。

(二) **檢視相關規範並適時進行法規調適**

(三) **利用 AI 技術發展監理科技**

(四) **與國際組織及其他國家金融監理機關進行交流及合作**

(五) **鼓勵金融業積極參與 AI 的研發與應用及協助導入最佳實務做法**

(六) **檢視金融業者應用 AI 之實際狀況**

(七) **責成各金融業公會制訂金融業運用 AI 系統相關自律規範及最佳實務守則**

(八) **督導金融機構落實公平對待客戶及金融友善準則，以及透過金融知識宣導活動降低數位落差**

金管會表示，「金融業運用 AI 指引」（草案）係行政指導，目的在「提醒」金融業者於導入或運用 AI 時宜注意的事項，而非「要求」金融業完全依照指引辦理。該指引（草案）亦強調金融機構宜視本身業務及應用 AI 的情形，以風險為基礎，參考指引所提醒的事項是否已進行評估。