英國資訊委員辦公室提出人工智慧（AI）稽核框架

人工智慧（Artificial Intelligence, AI）的應用，已逐漸滲透到日常生活各領域中。為提升AI運用之效益，減少AI對個人與社會帶來之負面衝擊，英國資訊委員辦公室（Information Commissioner's Office, ICO）於2019年3月提出「AI稽核框架」（Auditing Framework for Artificial Intelligence），作為確保AI應用合乎規範要求的方法論，並藉機引導公務機關和企業組織，評估與管理AI應用對資料保護之風險，進而建構一個可信賴的AI應用環境。

AI稽核框架主要由二大面向所構成—「治理與可歸責性」（governance and accountability）以及「AI特定風險領域」（AI-specific risk areas）。「治理與可歸責性」面向，係就公務機關和企業組織，應採取措施以遵循資料保護規範要求的角度切入，提出八項稽核重點，包括：風險偏好（risk appetite）、設計階段納入資料保護及透過預設保護資料（data protection by design and by default）、領導管理與監督（leadership management and oversight）、政策與程序（policies and procedures）、管理與通報架構（management and reporting structures）、文書作業與稽核紀錄（documentation and audit trails）、遵循與確保能力（compliance and assurance capabilities）、教育訓練與意識（training and awareness）。

「AI特定風險領域」面向，則是ICO特別針對AI，盤點下列八項潛在的資料保護風險，作為風險管理之關注重點：

一、 資料側寫之公平性與透明性（fairness and transparency in profiling）；

二、 準確性（accuracy）：包含AI開發過程中資料使用之準確性，以及應用AI所衍生資料之準確性；

三、 完全自動化決策模型（fully automated decision making models）：涉及人類介入AI決策之程度，歐盟一般資料保護規則（General Data Protection Regulation, GDPR）原則上禁止無人為介入的單純自動化決策；

四、 安全性與網路（security and cyber）：包括AI測試、委外處理資料、資料重新識別等風險；

五、 權衡（trade-offs）：不同規範原則之間的取捨，如隱私保護與資料準確性；

六、 資料最少化與目的限制（data minimization and purpose limitation）；

七、 資料當事人之權利行使（exercise of rights）；

八、 對廣泛公共利益和權利之衝擊（impact on broader public interests and rights）。

ICO將持續就前述AI特定風險領域，進行更深入的分析，並開放公眾討論，未來亦將提供相關技術和組織上之控制措施，供公務機關及企業組織進行稽核實務時之參考。

相關連結

- An Overview of the Auditing Framework for Artificial Intelligence and Its Core Components
- A Call for Participation: Building the ICO's Auditing Framework for Artificial Intelligence

你可能會想參加

→ 【2023科技法制變革論壇】AI生成時代所帶動的ChatGPT法制與產業新趨勢

→ 製造業及技術服務業個資保護及資安落實－經濟部工業局112年企業個人資料保護暨資訊安全宣導說明會

→ 【已額滿】2023科技研發法制推廣活動—科專個資及反詐騙實務講座

→ 「跨域數位協作與管理」講座活動

→ 新創採購-政府新創應用分享會

→ 【實體】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
→ 【線上】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
→ 數位發展部數位產業署113年資訊服務業安維計畫常見問題分享說明會
→ 【線上場】113年「新創採購機制及鼓勵照護機構參與推動」說明會
→ 【北部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【南部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 商業服務業個資保護宣導說明會
→ 個人資料保護新思維企業法遵論壇
→ 113年新創採購-照護機構獎勵說明會
→ 【南部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【北部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【中部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【實體】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
→ 【直播】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
→ 【臺北場】113年度新創採購-招標作業廠商說明會
→ 【臺中場】113年度新創採購-招標作業廠商說明會
→ 【高雄場】113年度新創採購-招標作業廠商說明會
→ 中部場–商業服務業個資保護工作坊
→ 南部場–商業服務業個資保護工作坊
→ 北部場–商業服務業個資保護工作坊
→ 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會

張腕純
組長 編譯整理

上稿時間：2019年06月

資料來源：
An Overview of the Auditing Framework for Artificial Intelligence and Its Core Components, AI Auditing Framework Blog, (Mar. 26, 2019), https://ai-auditingframework.blogspot.com/2019/03/an-overview-of-auditing-framework-for_26.html (last visited May 3, 2019).
A Call for Participation: Building the ICO's Auditing Framework for Artificial Intelligence, AI Auditing Framework Blog, (Mar. 18, 2019), https://ai-auditingframework.blogspot.com/2019/03/simon-mcdougall-director-for-technology.html (last visited May 3, 2019).

文章標籤

人工智慧 巨量資料 個人資料 隱私保護 資料運用

推薦文章