

數據保護、職業保密與雲服務

Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland), Solicitor (Hong Kong),
Solicitor (England & Wales)

人工智能依賴數據。巴塞爾各金融機構所持有的數據中，有很大一部分受法律保護。經修訂的《聯邦數據保護法》（FADP）自 2023 年 9 月 1 日起施行，適用於私人和聯邦機構對個人數據的處理。該法在技術上保持中立，因此雖未明確提及人工智能系統，卻同樣涵蓋這些系統。聯邦數據保護和資訊專員（FDPIC）在 2023 年 11 月的一份聲明中確認了這一點，提醒提供者和使用者：現行法律直接適用於人工智能支持的數據處理。¹在實踐中，有三項條款最為重要。第 21 條規定，如果某項完全基於自動化處理作出的決定產生法律效果或對當事人造成重大影響，數據控制者須告知數據主體，數據主體可要求由自然人對該決定進行復核。第 22 條規定，凡數據處理可能對數據主體的人格或基本權利造成高風險的，須進行數據保護影響評估。第 16 條規範向境外披露數據的行為，一旦模型在瑞士境外的伺服器上運行，這一條款便具有現實意義。

2

銀行保密又增加了一層刑法維度。《銀行法》（BankA）第 47 條規定，凡以銀行高級職員、僱員、代理人或清算人身份獲知秘密而予以洩露者，均應受到處罰。E 部分第四章已經指出，這一條款在銀行保密對外國稅務機關終結之後依然存續，並仍保護客戶數據免遭未經授權地向私人第三方披露。³因此，銀行若將客戶數據發送給外部人工智能提供者，必須確保該提供者負有保密義務，

其人員的訪問受到限制和控制，且這些數據不得用於訓練供他人使用的模型。瑞士金融市場監管局（FINMA）關於外包的通函還就服務提供者的選擇、指示和監督，以及銀行取回其數據和允許審計的能力提出了額外要求。⁴

在巴塞爾為客戶提供諮詢的律師、受託人及其他專業人士也負有相應的義務。《瑞士刑法典》（StGB）第 321 條保護委託給律師、醫生及某些其他職業人員的客戶秘密，而《聯邦律師自由執業法》（BGFA）第 13 條則規定了職業保密義務。J 部分第四章曾結合機器翻譯討論過這些條款。同樣的分析適用於每一種被輸入客戶資訊的人工智能工具。⁵各職業的實際解決方案大同小異：使用託管於瑞士或受控環境中的工具，以合同排除利用客戶數據進行訓練，儘可能進行匿名化處理，並在風險需要時取得客戶的知情同意。

模型在何處運行的問題已帶有政治色彩。大型人工智能模型和雲基礎設施的提供者均設在美國，而美國 2018 年的《澄清境外合法使用數據法》（CLOUD Act）允許美國當局要求受其管轄的提供者披露存儲在境外的數據。瑞士銀行以合同和技術保障措施作為應對，例如採用由瑞士境內持有密鑰的加密方式，同時已有多家提供者在瑞士建立了數據中心。⁶這些措施降低了風險，但並未消除風險，這也解釋了人們為何對瑞士模型和瑞士基礎設施抱有興趣，下文的第三種情景將對此加以探討。

1 註釋

1. 《聯邦數據保護法》（FADP，SR 235.1），自 2023 年 9 月 1 日起施行；聯邦數據保護和資訊專員（FDPIC），關於 FADP 對人工智能適用性的聲明，2023 年 11 月 9 日。有待核實。
2. FADP 第 16 條、第 21 條和第 22 條。有待核實。

3. 《銀行法》（BankA，SR 952.0）第 47 條；參見 E 部分第四章。有待核實。
4. FINMA 第 2018/3 號通函《外包》，關於服務提供者的選擇、指示和控制、數據安全以及審計權的邊碼。有待核實。
5. 《瑞士刑法典》（StGB，SR 311.0）第 321 條；《聯邦律師自由執業法》（BGFA，SR 935.61）第 13 條；參見 J 部分第四章關於機器翻譯、人工智能與職業保密的一節。有待核實。
6. 美國《澄清境外合法使用數據法》（Clarifying Lawful Overseas Use of Data Act，CLOUD Act），2018 年 3 月 23 日頒佈；關於瑞士銀行使用雲服務的情況，參見瑞士銀行家協會，Cloud Guidelines（2019 年第一版，其後有修訂版）。現狀有待核實。

僅供一般參考。本文不構成法律或稅務意見，不能取代針對個別情況的專業意見，亦不建立律師與客戶關係。本文反映截至 2026 年 9 月的法律狀況。

網上版本：hk.helveticaregister.com/basel-data-protection-professional-secrecy-and-the-cloud