

数据保护、职业保密与云服务

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

人工智能依赖数据。巴塞尔各金融机构所持有的数据中，有很大一部分受法律保护。经修订的《联邦数据保护法》（FADP）自 2023 年 9 月 1 日起施行，适用于私人 and 联邦机构对个人数据的处理。该法在技术上保持中立，因此虽未明确提及人工智能系统，却同样涵盖这些系统。联邦数据保护和信息专员（FDPIC）在 2023 年 11 月的一份声明中确认了这一点，提醒提供者和使用者：现行法律直接适用于人工智能支持的数据处理。¹在实践中，有三项条款最为重要。第 21 条规定，如果某项完全基于自动化处理作出的决定产生法律效果或对当事人造成重大影响，数据控制者须告知数据主体，数据主体可要求由自然人对该决定进行复核。第 22 条规定，凡数据处理可能对数据主体的人格或基本权利造成高风险的，须进行数据保护影响评估。第 16 条规范向境外披露数据的行为，一旦模型在瑞士境外的服务器上运行，这一条款便具有现实意义。

2

银行保密又增加了一层刑法维度。《银行法》（BankA）第 47 条规定，凡以银行高级职员、雇员、代理人或清算人身份获知秘密而予以泄露者，均应受到处罚。E 部分第四章已经指出，这一条款在银行保密对外国税务机关终结之后依然存续，并仍保护客户数据免遭未经授权地向私人第三方披露。³因此，银行若将客户数据发送给外部人工智能提供者，必须确保该提供者负有保密义务，

其人员的访问受到限制和控制，且这些数据不得用于训练供他人使用的模型。瑞士金融市场监管局（FINMA）关于外包的通函还就服务提供者的选择、指示和监督，以及银行取回其数据和允许审计的能力提出了额外要求。⁴

在巴塞尔为客户提供咨询的律师、受托人及其他专业人士也负有相应的义务。《瑞士刑法典》（StGB）第 321 条保护委托给律师、医生及某些其他职业人员的客户秘密，而《联邦律师自由执业法》（BGFA）第 13 条则规定了职业保密义务。J 部分第四章曾结合机器翻译讨论过这些条款。同样的分析适用于每一种被输入客户信息的人工智能工具。⁵各职业的实际解决方案大同小异：使用托管于瑞士或受控环境中的工具，以合同排除利用客户数据进行训练，尽可能进行匿名化处理，并在风险需要时取得客户的知情同意。

模型在何处运行的问题已带有政治色彩。大型人工智能模型和云基础设施的提供者均设在美国，而美国 2018 年的《澄清境外合法使用数据法》（CLOUD Act）允许美国当局要求受其管辖的提供者披露存储在境外的数据。瑞士银行以合同和技术保障措施作为应对，例如采用由瑞士境内持有密钥的加密方式，同时已有多家提供者在瑞士建立了数据中心。⁶这些措施降低了风险，但并未消除风险，这也解释了人们为何对瑞士模型和瑞士基础设施抱有兴趣，下文的第三种情景将对此加以探讨。

1 注释

1. 《联邦数据保护法》（FADP, SR 235.1），自 2023 年 9 月 1 日起施行；联邦数据保护和信息专员（FDPIC），关于 FADP 对人工智能适用性的声明，2023 年 11 月 9 日。有待核实。
2. FADP 第 16 条、第 21 条和第 22 条。有待核实。

3. 《银行法》（BankA, SR 952.0）第 47 条；参见 E 部分第四章。有待核实。
4. FINMA 第 2018/3 号通函《外包》，关于服务提供者的选择、指示和控制、数据安全以及审计权的边码。有待核实。
5. 《瑞士刑法典》（StGB, SR 311.0）第 321 条；《联邦律师自由执业法》（BGFA, SR 935.61）第 13 条；参见 J 部分第四章关于机器翻译、人工智能与职业保密的一节。有待核实。
6. 美国《澄清境外合法使用数据法》（Clarifying Lawful Overseas Use of Data Act, CLOUD Act），2018 年 3 月 23 日颁布；关于瑞士银行使用云服务的情况，参见瑞士银行家协会，Cloud Guidelines（2019 年第一版，其后有修订版）。现状有待核实。

仅供一般参考。本文不构成法律或税务意见，不能替代针对个案的专业意见，亦不建立律师与客户关系。本文反映截至 2026 年 9 月的法律状况。

在线版本: cn.helveticaregister.com/basel-data-protection-professional-secrecy-and-the-cloud