

Data protection, professional secrecy and the cloud

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

Artificial intelligence depends on data. Much of the data held by Basel's financial institutions is protected by law. The revised Federal Act on Data Protection, in force since 1 September 2023, applies to the processing of personal data by private persons and federal bodies. It is technology-neutral and therefore covers AI systems without naming them. The Federal Data Protection and Information Commissioner confirmed this in a statement of November 2023, in which he reminded providers and users that the existing law applies directly to AI-supported processing.¹ Three provisions matter most in practice. Article 21 obliges the controller to inform the data subject of a decision based exclusively on automated processing that produces a legal effect or significantly affects the person, allowing the data subject to have the decision reviewed by a natural person. Article 22 requires a data protection impact assessment where processing is likely to lead to a high risk for the personality or fundamental rights of the data subject. Article 16 governs the disclosure of data abroad, which becomes relevant whenever a model runs on servers outside Switzerland.²

Banking secrecy adds a criminal law dimension. Article 47 of the Banking Act punishes anyone who discloses a secret entrusted to them in their capacity as an officer, employee, agent or liquidator of a bank. Part E, Chapter IV showed that this provision survived the end of banking secrecy for foreign tax authorities and still protects client data against unauthorised disclosure to private third parties.³ A bank that sends client data to an external AI provider must therefore ensure that the provider is bound by confidentiality, that access by its personnel is restricted and controlled and that the data cannot be used to train models available to others. FINMA's outsourcing circular adds requirements on the selection, instruction and monitoring of the service provider and on the bank's ability to retrieve its data and to allow audits.⁴

Lawyers, trustees and other professionals who advise clients in Basel face corresponding obligations. Article 321 of the Swiss Criminal Code protects the secrets of clients entrusted to lawyers, doctors and certain other professions, while Article 13 of the Federal Act on the Free Movement of Lawyers imposes professional confidentiality. Part J, Chapter IV discussed these provisions in connection with machine translation. The same analysis applies to every AI tool into which client information is entered.⁵ The practical solutions are similar across professions: tools hosted in Switzerland or in a controlled environment, contractual exclusion of training on client data, anonymisation where possible and the client's informed consent where the risk requires it.

The question of where models run has acquired a political dimension. The large providers of AI models and cloud infrastructure are based in the United States, whose CLOUD Act of 2018 allows American authorities to require providers under their jurisdiction to disclose data stored abroad. Swiss banks have responded with contractual and technical safeguards, such as encryption with keys held in Switzerland, while several providers have built data centres in the country.⁶ These measures reduce the risk without removing it, which explains the interest in Swiss models and Swiss infrastructure that the third scenario below considers.

1 Notes

1. Federal Act on Data Protection (FADP, SR 235.1), in force since 1 September 2023; Federal Data Protection and Information Commissioner (FDPIC), statement on the applicability of the FADP to AI, 9 November 2023. To be verified. ↩
2. Arts. 16, 21 and 22 FADP. To be verified. ↩
3. Art. 47 of the Banking Act (BankA, SR 952.0); see Part E, Chapter IV. To be verified. ↩
4. FINMA Circular 2018/3 Outsourcing, margin numbers on selection, instruction and control of the service provider, data security and audit rights. To be verified. ↩
5. Art. 321 of the Swiss Criminal Code (StGB, SR 311.0); Art. 13 of the Federal Act on the Free Movement of Lawyers (BGFA, SR 935.61); see Part J, Chapter IV, section on machine translation, AI and professional secrecy. To be verified. ↩

6. United States Clarifying Lawful Overseas Use of Data Act (CLOUD Act), enacted 23 March 2018; on Swiss banks' use of cloud services, see the Swiss Bankers Association, Cloud Guidelines (first edition 2019, revised editions thereafter). Status to be verified. ↩

For general information only. This article does not constitute legal or tax advice, does not replace advice on an individual case and creates no lawyer-client relationship. It reflects the legal position as of September 2026.

Online version: helveticaregister.com/basel-data-protection-professional-secrecy-and-the-cloud