

Banking secrecy and professional secrecy

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

For banks, the FADP is overlaid by banking secrecy. Art. 47 of the Banking Act makes it a criminal offence for bank organs, employees, agents and auditors to disclose secrets entrusted to them in that capacity.¹ The protection extends to client data processed in IT systems and therefore to data that a bank feeds into an artificial intelligence system, whether its own or that of a provider. Disclosure to a service provider is not an offence if the provider is bound by secrecy and acts as an auxiliary of the bank within the framework of outsourcing. Disclosure to a provider abroad, whose staff could be compelled by foreign authorities to produce the data, raises questions that the banks have answered through contractual and technical measures such as encryption, pseudonymization and the retention of keys in Switzerland. The Swiss Bankers Association's guidelines on the use of cloud services set out the industry's approach.² Asset managers, trustees and fiduciaries are subject to the professional secrecy rules of the Financial Institutions Act (Art. 69 FinIA), and lawyers and fiduciaries in Ticino to their own professional secrecy.³

Generative artificial intelligence gives the issue a new practical urgency. An employee who copies a client letter into a public chatbot discloses the client's data to the provider of the chatbot, which may store it on servers abroad and may use it to train its models. Many Lugano institutions have therefore prohibited the use of public chatbots for client data and introduced enterprise versions with contractual guarantees, or models that run on their own infrastructure or on a Swiss platform. The release of Apertus by the Swiss AI Initiative, described above, and its availability through a Swiss telecommunications provider respond directly to this demand.⁴

1 Italian clients and the GDPR

Most of the clients of Lugano banks and asset managers live in Italy. The GDPR applies to a controller outside the European Union when it processes personal data of data subjects in the Union in connection with offering them goods or services or monitoring their behaviour (Art. 3(2) GDPR).⁵ Whether a Lugano bank "offers" services to Italian residents in this sense depends on the facts, and the analysis overlaps with the question of cross-border financial services treated in Chapter E.IV. A bank that actively markets its services in Italy is likely to be subject to the GDPR for these clients and may have to designate in writing a representative in the Union (Art. 27(1) GDPR). The duty lapses only for processing that is occasional, does not include largescale processing of special categories of data or of data on criminal convictions and is unlikely to result in a risk to the data subjects (Art. 27(2) GDPR), an exception that a bank with a regular Italian clientele will rarely be able to invoke. A bank that serves Italian clients only on their own initiative, in Switzerland, has a better argument that it is outside the scope. In either case the European Commission has recognized Switzerland as providing an adequate level of protection, a finding first made in Decision 2000/518/EC of 26 July 2000 and confirmed in the Commission's review of 15 January 2024, so that data can flow from Italy to Switzerland without additional safeguards.⁶

The Italian data protection authority, the *Garante per la protezione dei dati personali*, has been among the most active European authorities on artificial intelligence. By an urgent decision of 30 March 2023 it temporarily limited the processing of Italian users' data by ChatGPT. When it closed its investigation in December 2024, it fined the provider EUR 15 million for violations of the GDPR, among them the processing of data for training without an adequate legal basis, deficient transparency, the failure to notify a data breach of March 2023 and the absence of age verification, and it ordered OpenAI to run a six-month information campaign in Italian media.⁷ For Lugano institutions with Italian clients, the practice of the Garante is a reminder that the use of artificial intelligence on data of Italian residents may be scrutinized under Italian and European standards, which are in several respects stricter than the Swiss ones.

Essentials. The revised FADP, in force since 1 September 2023, applies directly to artificial intelligence. Its key provisions for financial institutions are privacy by design (Art. 7), processors (Art. 9), disclosure abroad (Art. 16–17), automated individual decisions (Art. 21), impact assessments (Art. 22) and breach notification (Art. 24). Banking secrecy under Art. 47 BankA and professional secrecy under Art. 69 FinIA add criminal protection of

client data. For clients in Italy the GDPR may apply under its Art. 3(2), and the Italian Garante enforces it actively in the field of artificial intelligence.

2 Notes

1. Banking Act (above), Art. 47 para. 1 (organs, employees, agents, liquidators and employees of audit firms who disclose a secret entrusted to them in that capacity; custodial sentence of up to three years or a monetary penalty), <https://www.droit-bilingue.ch/de-fr/9/95/952.0-47-100.html>. ↩
2. Swiss Bankers Association, Cloud Guidelines (first edition March 2019, later updated). ↩
3. FinIA (above), Art. 69 ("Verletzung des Berufsgeheimnisses": custodial sentence of up to three years or a monetary penalty), <https://www.droit-bilingue.ch/de-fr/9/95/954.1-69-72.html>; for fiduciaries in Ticino see Chapter E.III. ↩
4. EPFL AI Center (2 September 2025, above) (Swisscom as strategic partner; Swiss sovereign AI platform). ↩
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1, <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>; text of Art. 3(2) and Art. 27(1)–(2) consulted at <https://gdpr-info.eu/art-3-gdpr/> and <https://gdpr-info.eu/art-27-gdpr/>. ↩
6. European Commission, Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, COM(2024) 7 final, Brussels, 15 January 2024, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52024DC0007> ("Switzerland continues to provide an adequate level of protection for personal data transferred from the EU"); Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC on the adequate protection of personal data provided in Switzerland, C(2000) 2304, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000D0518>. ↩

Banking secrecy and professional secrecy

7. Garante per la protezione dei dati personali, Provvedimento n. 112 of 30 March 2023 (urgent temporary limitation of processing against OpenAI L.L.C.), <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870832>; Garante, press release "ChatGPT, il Garante privacy chiude l'istruttoria" (20 December 2024), on Provvedimento n. 755 of 2 November 2024 (fine of EUR 15 million, six-month information campaign, transfer of continuing proceedings to the Irish authority as lead authority), <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10085432>. ↩

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/lugano-banking-secrecy-and-professional-secrecy