THOMSON REUTERS
PRACTICAL LAW™

Bank Secrecy Laws (Switzerland)

by Alexander Hofmann, LAUX LAWYERS AG, with Practical Law Data Privacy & Cybersecurity

Status: **Law stated as of 24 Mar 2022** | Jurisdiction: **Switzerland**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/w-010-8058**
Request a free trial and demonstration at: **us.practicallaw.tr.com/about/freetrial**

A Practice Note discussing the laws, regulations, and guidance governing bank secrecy in Switzerland including the Swiss Federal Act on Banks and Savings Banks and guidance issued by Switzerland's financial regulator, the Swiss Financial Market Supervisory Authority. This Note provides guidance for banking institutions handling customer data in Switzerland on complying with bank secrecy obligations, the circumstances in which they can disclose customer data to third parties, and required steps to permit disclosure. This Note also discusses the Federal Act on Data Protection, the Ordinance to the Federal Act on Data Protection, and how banks should address data protection obligations when handling customers' personal data.

Bank secrecy laws generally prohibit banking institutions, and their officers and employees, from disclosing customer data to third parties. However, banks commonly need to disclose customer data for routine business purposes including:

- Providing products and services to customers.
- Making inter-company transfers.
- Outsourcing to third-party service providers.
- Responding to litigation and regulatory inquiries.

Global banks operating in jurisdictions with bank secrecy laws must find practical solutions to perform business functions or face sanctions. Potential sanctions include fines, regulatory actions, and in severe cases, criminal penalties for disclosing customer data in violation of bank secrecy laws.

This Note discusses the laws and regulations governing bank secrecy in Switzerland. It provides guidance for banking institutions handling customer data in Switzerland on complying with bank secrecy obligations, the circumstances in which banks can disclose customer data to third parties, and required steps to permit disclosure. This Note also discusses the Swiss data protection law and how banks should address data protection obligations when handling customers' personal data.

For information on global bank secrecy laws, see Practice Note, Global Bank Secrecy Laws: Overview and Global Bank Secrecy Toolkit.

Customer Data Disclosure Laws

Article 47 of the Swiss Federal Act on Banks and Savings Banks (Banking Act) is the primary law governing bank secrecy in Switzerland. Those disclosing customer data in violation of this provision face criminal penalties (see Enforcement and Penalties).

Similar criminal provisions exist in other Swiss financial market laws including:

- Article 69 of the Swiss Federal Act on Financial Institutions. This imposes professional secrecy obligations on directors, officers, employees, agents, and liquidators of financial institutions. Financial institutions include portfolio managers, trustees, managers of collective assets, fund management companies and securities firms.
- Article 147 of the Swiss Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading. This imposes professional secrecy obligations on directors, officers, employees, agents, and liquidators of financial market infrastructures. Financial market infrastructures include stock exchanges, multilateral trading facilities, central counterparties, central securities depositories, trade repositories, and payments systems.

Swiss banks also have a civil obligation regarding the confidentiality of customer data which arises out of:

- **The civil right to personal privacy**. Article 28 of the Swiss Civil Code recognizes individuals' and companies'

right to privacy, including economic privacy and information on their banking relationships and the assets concerned.

- **The contractual relationship between the customer and the bank.** Under Article 398 of the Swiss Code of Obligations agents are liable to principals for the diligent and faithful performance of the business entrusted to them. This obligates banks to keep customer data entrusted to it confidential.

This Note focuses primarily on a bank's obligations under the Banking Act. Other criminal and civil laws are outside the scope of this Note.

Covered Persons and Entities

Banks Covered

The banking secrecy provisions in Article 47 apply to the following entities:

- Banks licensed in Switzerland.
- Established branches or representative offices of foreign banks in Switzerland.
- Private banks in Switzerland (banks in the legal form of individual proprietorships or general and limited partnerships).
- Saving banks in Switzerland.

(Articles 1(1) and 2(1), Banking Act.)

Article 1a of the Banking Act defines banks as companies active mainly in the financial sector that perform any of the following:

- Accept deposits from the public.
- Finance their own accounts or the accounts of third parties with loans from banks that do not own any significant holdings in them.

The Banking Act does not apply to:

- Stockbrokers and trading houses dealing only in securities and directly related transactions if they do not conduct the banking activities described above.
- Asset managers, public notaries, and business agents who limit their activities to managing their clients' assets without conducting the above banking activity.

(Article 1(3), Banking Act.)

The Banking Act does not extend to banks located overseas that handle Swiss residents' customer data.

Individuals Covered

Article 47 of the Banking Act broadly prohibits any individuals from disclosing customer data entrusted to them or observed in their capacity as:

- A member of an executive or supervisory body of the bank.
- An employee or representative of the bank.
- A liquidator of a bank.
- A member of a body or employee of an audit firm.

(Article 47(1)(a), Banking Act.)

Bank secrecy obligations exist even after revocation of a bank license or termination of an individual's official responsibilities (Article 47(4), Banking Act).

Criminal penalties may apply for Article 47 bank secrecy violations when data is disclosed in Switzerland or abroad (Article 8(1), Swiss Criminal Code) (stating that a crime takes place where the offender acts and where the consequences occurred)).

Protected Customer Data

Article 47 of the Banking Act does not specify the scope of customer data protected from disclosure and broadly precludes the disclosure of confidential information entrusted to covered persons and entities. This language covers all data stemming from the business relationship between the bank and customer including:

- Information on the customer as a private individual.
- Deposits and withdrawals.
- Loan information.
- Value of investments.
- Information in banking agreements.
- Information requests and offerings for further financial services.
- Information given by customers about their financial circumstances.
- The customer's relationship with other banks, if any.
- The bank's own transactions, if disclosure would harm a customer.
- Transactions between different banks (which then become customers vis à vis each other).
- Information about third-party customers the bank received in the course of its business activities.

The Banking Act only protects information related to an identified or identifiable customer. A bank can therefore disclose customer data by, for example, effectively anonymizing the customer name, account number, online identifier, or other identifying information, or by aggregating customer data.

The Swiss Financial Market Supervisory Authority (FINMA) provided guidance on the scope of customer data when discussing confidentiality and security requirements in FINMA Circular 2008/21 (FINMA Circular 2008/21). FINMA Circular 2008/21 states that customer identifying data includes direct and indirect customer identification data such as:

- Name (first name, second name, and family name).
- Passport number.
- A combination of indirect customer identification data that together may identify a specific customer (for example, a combination of birth, profession, and nationality data).

(Annex 3, FINMA Circular 2008/21.)

FINMA Circular 2008/21 states that when anonymizing customer personal data, the bank should remove or permanently change (through, for example, deletion or aggregation) all elements that could allow identification of a person (Annex 3, FINMA Circular 2008/21, at 35).

Principles for Managing Customer Data

Banks covered by the Banking Act must comply with FINMA's guidance for securing and handling customer data. FINMA Circular 2008/21 sets out principles on the proper management of risks related to electronic customer data. The principles include:

- **Governance risks.** Banks must systematically identify, mitigate, and monitor risks in connection with customer data. An independent unit must exercise control over creating a security framework.
- **Data classification.** Banks must categorize customer data according to confidentiality levels and the protection required. Units responsible for customer data must monitor the entire life cycle of customer data, including access right approvals and deletion and disposal of backup and operational systems.
- **Data inventory.** Banks must maintain an inventory of:
  - where they store customer data;
  - the applications and IT-systems used for processing; and
  - which national and international locations can access data (including outsourced services and external firms).

  Banks must adequately protect customer data stored or accessible from outside of Switzerland through, for example, anonymization, encryption, or pseudonymization.
- **Data security.** Banks should implement security standards for infrastructure and technology used to protect the confidentiality of customer data. The bank should compare the security standards to market practice on a regular basis to identify security gaps. Banks should consider independent reviews and audit reports when developing security standards.
- **Employee training.** Banks must train and monitor employees and third parties with access to customer data regularly (see Outsourcing Considerations). The bank should maintain a list of all internal and external information technology (IT) users that have access to mass customer data (key employees only).
- **Risk identification and control.** The bank unit responsible for data security and confidentiality must identify and evaluate inherent risks regarding customer data confidentiality using a structured process. The bank must involve the business, IT, and control functions in the process.
- **Risk mitigation.** Banks must monitor and minimize risks pertaining to data processing activities when it modifies or migrates large quantities of customer data.
- **Incidents related to confidentiality of customer data.** Banks should introduce predefined processes to react swiftly to confidentiality incidents, including a clear strategy on how to communicate serious incidents. Banks must monitor, analyze, and share with executive management exceptions, incidents, and audit results.
- **Outsourcing services.** Banks must conduct due diligence on whether a third-party service provider can adequately protect customer data (see Outsourcing Considerations).

(Annex 3, FINMA Circular 2008/21.)

Banking Act Exceptions Permitting Disclosure

Several Banking Act exceptions allow banks to disclose otherwise protected customer data. Permissible disclosures include those banks make:

- When requested under a Swiss statute requiring disclosure of information to a government authority (Article 47(5), Banking Act).

- To a parent company that a banking or financial market supervisory authority regulates if the disclosure is necessary for consolidated supervision purposes provided that:
  - the information is used exclusively for internal control or direct supervision of banks or other licensed financial intermediaries;
  - official secrecy or professional confidentiality obligations bind the parent company and supervisory authority responsible for consolidated supervision; and
  - the information is not transmitted to third parties without the prior permission of the bank or based on the blanket permission previously defined in a state treaty.

  (Article 4^{quinquies}, Banking Act.)
- In cases of an overriding private or public interest (see, for example, Article 17, Swiss Criminal Code and Article 28^{30}(2), Swiss Civil Code, which permit banks to disclose protected data when there is an overriding interest). Overriding private interests include, for example:
  - disclosure to debt collection companies; and
  - solvency checks and credit assessments.

  (See also, for example, Swiss Federal Court Judgment No 137 II 431 (15 July 2011) (court discussed overriding public interest as a legal basis to disclose customer data to US regulators).)
- To comply with a bank's reporting obligations under Swiss law including laws that require banks to:
  - provide FINMA with all information and documents that it requires to carry out its tasks (Article 29, Federal Act on the Swiss Financial Market Supervisory Authority (June 22, 2007)) (FINMASA));
  - immediately report to FINMA any incident of substantial importance to the bank's supervision (Article 29, FINMASA); and
  - report to the Money Laundering Reporting Office Switzerland when it knows or reasonably suspects that assets involved in the business relationship with a bank customer are the proceeds of a crime or serve the financing of terrorism (Article 9, Swiss Federal Act on Combating Money Laundering and Terrorist Financing).
- To comply with agreements Switzerland has entered into with other countries, including:
  - the OECD Model Tax Convention which permits the exchange of bank customer data between competent authorities of the contracting countries if requested in cases of tax fraud and tax evasion;
  - the Agreement on the Automatic Exchange of Information (AEOI) which permits the automatic exchange of bank data on foreign customers between signatory countries to help fight tax evasion; and
  - the Agreement between the US and Switzerland for Cooperation to Facilitate the Implementation of FATCA (Foreign Account Tax Compliance Act) and the respective Swiss implementation law. This requires Swiss banks to provide US tax authorities with requested account information, either with affected customer's consent, or on an anonymous and aggregated basis.

Article 47 of the Banking Act does not specifically permit disclosure with customer consent but banks commonly obtain customer consent for needed disclosures not permitted under the Banking Act (see Customer Consent for Disclosures).

Disclosure in Litigation and Discovery

In Swiss civil proceedings, parties to the proceedings and third parties generally have a duty to cooperate in the evidentiary process. However, persons and entities bound by bank secrecy obligations may refuse to cooperate if they demonstrate that bank secrecy interests outweigh the interest in establishing the truth (Articles 163(2) and 166(2), Swiss Civil Procedure Code). For civil proceedings abroad, the Hague Convention on the Taking of Evidence Abroad applies and on request, a Swiss court may take the requested evidence.

In Swiss criminal proceedings, persons bound by bank secrecy must provide requested information or testify. The person responsible for directing the criminal proceeding may relieve them of the duty to testify if they establish that the interest in preserving confidentiality outweighs the interest in establishing the truth (Article 173(2), Swiss Criminal Procedure Code).

For criminal proceedings abroad, mutual assistance may be rendered to foreign states based on international treaties and the Swiss Federal Act on International Mutual Assistance in Criminal Matters. Swiss authorities will not lift bank customer secrecy for a foreign investigation unless the conduct under investigation also qualifies as a criminal offense under Swiss law.

Customer Consent for Disclosures

Unlike most country's bank secrecy laws, the Banking Act does not explicitly allow for the disclosure of customer data with customer consent. However, the legal effect of customer consent to disclose data is that

an unlawful disclosure of customer data becomes lawful (see, for example, Article 28[30](2), Swiss Civil Code) ("An infringement is unlawful unless it is justified by the consent of the person whose rights are infringed or by an overriding private or public interest or by law").

Banks commonly obtain consent when the customer opens an account by requiring the customer to agree to the bank's standard terms and conditions and privacy policy. To ensure the customer understands the scope of disclosure, banks should:

- Place the consent clause in a clearly visible and prominent place.
- Clearly define the scope of consent.
- Provide the customer with sufficient information about the potential impact of consent.

A universal, general waiver of bank secrecy obligations violates the Swiss Civil Code (Article 27(2), Swiss Civil Code) (stating that "[n]o person may surrender his or her freedom or restrict the use of it to a degree which violates the law or public morals").

For more information on obtaining customer consent to disclose data under bank secrecy laws, see Standard Clause, Customer Terms and Conditions for Data Disclosure Under Bank Secrecy Laws.

Before obtaining customer consent, banks should document all disclosures the bank makes, or anticipates making, to third parties and compare this list to the exceptions provided in the Banking Act and under Swiss law. If the Banking Act or Swiss law permits the disclosure, banks do not need customer consent to disclose the data.

Data Protection Law

Data protection is mainly regulated by the Federal Act on Data Protection (FADP) and the Ordinance to the Federal Act on Data Protection (FADP Ordinance). The FADP contains:

- General data protection rules.
- Specific regulations on data processing by private-sector organizations, individuals, and federal bodies.
- Provisions relating to the Federal Data Protection and Information Commissioner (FDPIC), which is the body responsible for supervising data protection.

The FADP Ordinance clarifies certain aspects of the FADP. In particular, the FADP Ordinance details the:

- Measures that must be taken for the cross-border personal data disclosures.
- Functions and duties of data protection officers and the FDPIC.

On September 25, 2020, Switzerland's parliament adopted the Revised Federal Act on Data Protection (in German) (Revised FADP), which will replace the FADP and FADP Ordinance. The Revised FADP:

- Modernizes Swiss data protection law.
- Complies with the Protocol amending Convention 108 (CETS No. 223) (Convention 108+).
- Aligns Swiss data protection law with the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR).
- Maintains Switzerland's adequacy status granted by the European Commission to ensure the free flow of personal data between the EU and Switzerland.

The Revised FADP also aims to maintain Switzerland's adequacy status granted by the European Commission to ensure the free flow of personal data between the EU and Switzerland.

The Federal Council announced the entry into force of the Revised FADP on September 1, 2023. On June 23, 2021, the Federal Council published a preliminary draft of the revised Ordinance to the FADP (in German), which complements the Revised FADP and will enter into force at the same time. However, the public hearing to the Ordinance revealed widespread criticism which will likely lead to a further thorough revision before the entering into force.

For more information on Switzerland's data protection rules and principles, see Country Q&A, Data protection in Switzerland: overview.

Applicability and Jurisdictional Scope

The FADP:

- Regulates personal data processing by federal bodies, private-sector organizations, and individuals, subject to certain exemptions (Article 2, FADP).
- Protects personal data of living individuals and legal entities (Article 3(b), FADP).

Both controllers of the data file (known as data controllers in other jurisdictions) and data processors are subject to the FADP. A controller of a data file is defined as private persons or federal bodies that decide on the purpose and content of a data file. The FADP does not include a definition of data processor.

The Revised Federal Act on Data Protection (in German) (Revised FADP) will impose obligations on "responsible persons" (private individuals or federal bodies that control the purpose and means of processing) and will adopt the concept of a processor under the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) (Article 5, Revised FADP).

Categories of Personal Data

The FADP regulates:

- Personal data, which is defined as all information relating to an identified or identifiable person (Article 3(a), FADP).
- Personal data of living individuals and legal entities (Article 3(b), FADP).
- Sensitive personal data, which is data relating to:
  - racial origin;
  - religious, ideological, political, or trade union-related views or activities;
  - health;
  - sex life and sexual orientation;
  - social security measures; and
  - administrative or criminal proceedings and sanctions.

  (Article 3(c), FADP.)

The FADP does not apply to the processing of anonymized data.

The Revised FADP:

- Excludes legal entities from the data subject definition.
- Expands the definition of sensitive personal data to include biometric and genetic data.
- Refers to the term profiling, rather than personality profiles, to align with the corresponding GDPR.
- Applies to foreign companies operating in Switzerland and require certain of those companies to appoint a representative in Switzerland.

(Articles 3, 5, Revised FADP.)

Principles

The FADP imposes the following data protection principles on banks handling personal data:

- Banks must process personal data lawfully, in good faith, and proportionately, meaning the bank should limit the personal data processing to what is necessary for it to achieve the purpose of processing.
- Banks may only process personal data for the purposes:
  - indicated at the time of collection;
  - evident from the circumstances; or
  - provided for by applicable law.
- The collection of personal data and in particular the purpose of its processing must be evident to the data subject.

  (Article 4, FADP.)

In addition, the FADP requires banks processing customer personal data to:

- Ensure that it is correct and complete (Article 5, FADP).
- Protect it against unauthorized processing through adequate technical and organizational measures (Article 7, FADP).
- On request, notify the customer about personal data processing activities and provide the information specified in Article 8 of the FADP (Article 8, FADP).

Non-compliance with the above principles constitutes a violation of the data subject's privacy unless the processing is justified by:

- The data subject's consent (see Cross-Border Transfer Restrictions).
- A provision of Swiss law requiring or permitting the processing including for example, an obligation to disclose information under the Banking Act (see Banking Act Exceptions Permitting Disclosure).
- An overriding private or public interest (see Overriding Private or Public Interest).

(Article 13(1), FADP.)

Disclosure of personal data to third parties is generally lawful if the bank satisfies the FADP principles or an Article 13 legal basis. However, for disclosure of sensitive personal data to third parties, organizations must have a justification under Article 13, even if the organization discloses personal data in compliance with the general principles (Article 12(2)(c), FADP).

Consent Under the Data Protection Law

If a bank complies with the general data processing principles set out in the FADP (see Principles), the customer does not need to consent to the personal data processing. However, in the rare case that a bank relies on

customer consent to process personal data, the consent is valid only if the customer:

- Consents voluntarily.
- Consents in advance of the personal data processing.
- Receives adequate and clear information about the personal data processing.

(Article 4(5), FADP.)

The FADP does not require the customer to consent in writing. Therefore, consent given orally or via electronic means (for example, by mouse click) is generally deemed sufficient. However, the bank bears the burden of proving consent, so consent in an explicit and recordable format is recommended for evidentiary purposes.

Implicit consent is sufficient for personal data processing except when seeking consent to process sensitive personal data or personality profiles (Article 4(5), FADP). The FADP requires express consent for processing of sensitive personal data or personality profiles (a collection of personal data that permits an assessment of essential characteristics of the personality of a natural person).

A customer has the right to withdraw consent at any time, although such withdrawal will not usually be applied retrospectively.

Overriding Private or Public Interest

The FADP permits personal data processing without consent if justified by an overriding private or public interest. This means the bank processes:

- Personal data relating to the contractual party in direct connection with the conclusion or the performance of a contract.
- Competitor personal data without disclosing the data to third parties.
- Personal data to verify a person's creditworthiness if the personal data:
  - does not include sensitive personal data or personality profiles (a collection of personal data that permits an assessment of essential characteristics of the personality of a natural person); and
  - is only disclosed to third parties where necessary to conclude or perform a customer's contract.
- Personal data on a professional basis exclusively for publication in the edited section of a periodically published medium.
- Personal data for research, planning, and statistical purposes and publishes the results in a de-identified form.
- Personal data concerning a person of public interest, provided the data relates to the public activities of that person.

(Article 13(2), FADP.)

Cross-Border Transfer Restrictions

The FADP restricts the transfer of personal data outside of Switzerland to countries that do not guarantee an adequate level of data protection (Article 6(1), FADP). The FDPIC has published a list (in French) of jurisdictions that it considers as providing adequate protection.

In the absence of legislation that guarantees adequate protection, banks can only transfer customer personal data outside of Switzerland if:

- The customer consents to the transfer.
- The bank establishes measures to ensure that it adequately protects personal data, by:
  - sufficient contractual guarantees; or
  - binding corporate rules if the transfer is between legal entities under common control.
- The processing is directly connected with the conclusion or the performance of a contract and the personal data concerns the customer.
- Disclosure is essential to either safeguard an overriding public interest or for the establishment, exercise, or enforcement of legal claims before the courts.
- Disclosure is required to protect the customer's life or the physical integrity of the data subject.
- The customer has made the personal data generally accessible and has not expressly prohibited its processing.

(Articles 6(1) and 6(2), FADP.)

The bank must notify the FDPIC when it transfers personal data to a non-adequate jurisdiction using any safeguards used to protect the personal data, such as data transfer agreements or binding corporate rules (Article 6(3), FADP; Article 6(1), FADP Ordinance). The obligation to provide information is fulfilled if:

The parties transfer data based on model contracts or standard contractual clauses (SCCs) that the FDPIC has approved.

The bank informs the FDPIC in general terms about the use of these model contracts or SCCs.

(Article 6(1)(3), FADP Ordinance.)

In September 2020, the FDPIC issued a position statement stating that the Swiss-US Privacy Shield does not offer an adequate level of protection for cross-border personal data transfers from Switzerland to the US under the FADP (see Legal update: archive, Swiss DPA Finds Swiss-US Privacy Shield Offers Inadequate Data Protection). The statement follows the European Court of Justice (ECJ) decision invalidating the EU-US Privacy Shield ((Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Case C-311/18) EU:C:2020:559) (Schrems II); see Legal update: case report, Schrems II: controller to processor standard contractual clauses valid but EU-US Privacy Shield invalid (ECJ)).

In June of 2021, the FDPIC released guidance to help organizations analyze the propriety of potential cross-border transfers.

On August 4, 2021, the FDPIC released a memorandum providing guidance for Swiss-domiciled entities registered with the US Securities and Exchange Commission (SEC) for transferring books and records containing personal data for the SEC's inspection and examination program. It also published a policy paper on the transfer of personal data to the US and other countries without an adequate level of data protection within the meaning of Article 6(1) of the FADP.

On August 27, 2021, the FDPIC issued:

A statement confirming that Swiss organizations may rely on the new EU SCCs approved by the European Commission on June 4, 2021, to legitimize personal data transfers from Switzerland to countries without an adequate level of data protection if the necessary amendments and adaptations are made for use under Swiss data protection law.

Transfer of personal data to a country with an adequate level of data protection based on recognised standard contractual clauses and model contracts guidance to help organizations make the necessary amendments and adaptations to the new EU SCCs.

For more information, see FDPIC: Transborder data flows (in French).

Customer Data Covered by the FADP and the Banking Act

Managing Compliance with Bank Secrecy and Data Protection Laws

Banks must conduct separate analyses of their customer data handling and compliance obligations under the Banking Act and FADP because these laws:

- Protect different categories of data.
- Apply in different circumstances.

For example:

- The FADP protects privacy in all areas and sectors and applies to any information identifying a natural or legal person, while the Banking Act protects a more limited set of data that includes customer account information when associated with a particular customer.
- The FADP broadly applies to the collection, processing, and cross-border transfer of broadly defined personal data while the Banking Act protects the disclosure of a bank's customer data.

Identifying Potential Conflicts Between the Bank Secrecy and Data Protection Laws

The Banking Act and the FADP serve the same purpose of protecting data from access by unauthorized third parties. The FADP also permits the processing and disclosure of personal data because the disclosure is authorized under another Swiss law, including the Banking Act. (Article 13(1), FADP) (see Banking Act Exceptions Permitting Disclosure).

However, banks may face a conflict if FADP allows disclosure of customer personal data in accordance with the general principles (see Principles) while the Banking Act prohibits disclosure.

Organizations should work with counsel to ensure that they comply with both the Banking Act and FADP requirements prior to disclosing customer data.

Outsourcing Considerations

Bank Secrecy Act Compliance in Outsourcing Arrangements

Outsourcing to a service provider is not considered an unlawful disclosure under Article 47 of the Banking Act if the bank obligates the outsourcing provider and its employees to comply with bank secrecy rules. The outsourcing provider and its employees may then be considered bank representatives under Article 47 and functionally integrated into the bank's organization.

However, banks outsourcing services to a third-party service provider remain accountable to FINMA in the same way as if performing the services themselves.

FINMA Circular 2018/3 sets out requirements for banks outsourcing services to third parties including requiring banks to:

- Maintain an inventory of the outsourced functions including a description of the outsourcing, the service provider, and the unit responsible for services within the outsourcing company.
- Conduct a risk analysis prior to retaining a third-party service provider and assign a responsible person within the bank to monitor and control the service provider.
- Specify the internal approval procedures for outsourcing projects and the responsibilities for signing outsourcing agreements.
- Enter into a written agreement with the service provider that:
  - grants the bank the right to instruct and control the service provider;
  - obligates the service provider to ensure performance continuation following an emergency;
  - requires the service provider to provide FINMA with all documentations on the outsourced function if the service provider is not supervised by FINMA;
  - grants the bank, its audit firm, and FINMA the right to inspect and audit information relating to the outsourced function at all times; and
  - requires the service provider to obtain approval to retain sub-contractors and bind them to the obligations in Circular 2018/3.
- Demonstrate that its external auditor under bank and stock-exchange laws and the FINMA can assume and legally enforce their auditing rights when outsourcing abroad.

Banks outsourcing services will also need to comply with Article 47 of the Banking Act, the FADP, and Annex 3 to FINMA Circular 2008/21 (see Principles for Managing Customer Data).

FADP

Under the FADP, banks may assign the personal data processing to third parties by agreement or by law if:

- The third-party service provider only processes the data in the manner allowed for by the instructing party.
- A statutory or contractual duty of confidentiality does not prohibit the assignment.
- The instructing party ensures that the third party guarantees data security.

(Article 10a, FADP.)

The bank remains responsible for complying with the FADP even when it retains a third-party service provider to process data. The bank should therefore select and instruct the service provider carefully and monitor the outsourcing relationship.

If the provider is located outside of Switzerland, the bank must also comply with the FADP's cross-border transfer requirements (see Cross-Border Transfer Restrictions).

Enforcement and Penalties

Bank Secrecy

Persons or entities disclosing customer data in violation of the Banking Act face:

- Criminal penalties (see Criminal Penalties).
- Administrative and civil measures (see Administrative and Civil Measures).
- Private lawsuits (see Private Lawsuits).

Criminal Penalties

Persons and entities intentionally violating Article 47 of the Banking Act face:

- Imprisonment of up to three years (Article 47(1), Banking Act).
- Imprisonment of up to five years if the violator enriches himself or others through the disclosure (Article 47(1bis), Banking Act).
- A monetary penalty under the Swiss Criminal Code based on a maximum of 360 daily penalty units. The court decides on the number of daily penalty units considering the culpability of the offender. A daily penalty unit amounts to a maximum of CHF3,000 The court decides on the value of the daily penalty unit according to the personal and financial circumstances of the offender at the time of conviction (Article 47(1), Banking Act and Article 34, Swiss Criminal Code).

For negligent violations of Article 47 of the Banking Act, violators face a criminal monetary penalty of up to CHF250,000 (Article 47(4), Banking Act).

There are only a few convictions annually under Article 47 Banking Act.

Administrative and Civil Measures

Violation of the bank secrecy obligation is a breach of financial markets law which can lead to administrative

measures under the Federal Act on the Swiss Financial Market Supervisory Authority (June 22, 2007) (FINMASA) including, but not limited, to:

- Withdrawal of the bank's license in the case of serious breach of a legal obligation (Article 37, FINMASA).
- Prohibiting the person responsible from acting in a management capacity at any entity subject to FINMA's supervision (Article 33, FINMASA).
- Issuance of a declaratory ruling when there is no longer a need to order measures to restore compliance with the law (Article 33, FINMASA).
- Publication in electronic or printed form of FINMA's final ruling (Article 34, FINMASA).
- Confiscation of any profit that a supervised person or entity or a responsible person in a management position made through the violation (Article 35, FINMASA).

Private Lawsuits

If the bank violates its contractual bank secrecy obligations owed to customers, it may be liable for damages under the general principles of Swiss contract law. The customer must prove the extent of financial damages suffered from the bank's infringement of contractual bank secrecy obligations. The bank has the burden of proving that it was not at fault (Article 97, Swiss Code of Obligation).

FADP

Persons and entities violating the FADP face the following penalties:

- **Criminal sanctions.** Under Article 35 of the FADP, anyone who does the following without authorization, is, on complaint, liable for a fine:
  - willfully discloses confidential, sensitive personal data, or personality profiles received in the course of their professional activities; or
  - willfully discloses confidential, sensitive personal data, or personality profiles that he obtains from a person bound by professional confidentiality.

  The unauthorized disclosure of confidential, sensitive personal data, or personality profiles remains an offense after termination of such professional activities or training.
- **Administrative proceedings.** The FDPIC can initiate investigations against persons and entities violating the FADP and issue non-binding recommendations. If a person or entity does not comply with or rejects a recommendation, the FDPIC may refer the matter to the Federal Administrative Court for decision. Under the Revised FADP, the FDPIC has the authority to issue regulations.
- **Data subject lawsuits.** Data subjects can request that:
  - data processing be stopped;
  - no data be disclosed to third parties; or
  - the personal data be corrected or destroyed.

(Article 15, FADP and Articles 28, Art. 28a, and 28l, Swiss Civil Code.)

The Revised FADP increases potential fines for breaches of data protection law (Articles 60 to 62, Revised FADP). However, unlike the GDPR, there will still be no administrative fines. Nevertheless, the scope of criminal sanctions will be widened.