Bank Secrecy Laws (Switzerland)

ALEXANDER HOFMANN, LAUX LAWYERS AG, WITHPRACTICAL LAW

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 a banking institution handling customer data in Switzerland on complying with bank secrecy obligations, the circumstances in which it can disclose customer data to third parties, and required steps to permit disclosure. This Note also discusses the Federal Act on Data Protection (19 June 1992). the Ordinance to the Federal Act on Data Protection (14 June 1993), 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, but not limited to:

- 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 including fines, regulatory actions, and in severe cases, criminal sanctions 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 (W-002-8052).

SWITZERLAND BANK SECRECY LEGAL FRAMEWORK

Article 47 of the Swiss Federal Act on Banks and Savings Banks (amended 2016) (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, in particular:

- Article 43 of the Swiss Federal Act on Stock Exchanges and Securities Trading. This imposes secrecy obligations on certain individuals and entities handling data received in connection with a stock exchange or securities dealer.
- Article 147 of the Swiss Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading. This obligates directors or officers, employees, agents, or liquidators of financial market infrastructures to not disclose confidential information. Financial market infrastructures include, for example, stock exchanges, multilateral trading facilities, central counterparties, central securities depositories, trade repositories, and payments systems.
- Article 148 of the Swiss Federal Act on Collective Investment Schemes. This imposes secrecy obligations on members of an executive or governing body, employees, agents, or liquidators of fund management companies.

Swiss banks also have a civil obligation to respect 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 an agent is liable to the principal for the diligent and faithful performance of the business entrusted to him. This obligates a bank 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 2 of the Ordinance on Banks and Savings Banks states that companies active mainly in the financial sector and that, in particular, perform the following banking activities shall be considered banks:

- Accept deposits from the public.
- Finance their own accounts or accounts of persons or companies with whom they do not form an economic entity 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 provided they do not conduct the banking activities described above.
- Private investment managers, public notaries, and business agents who limit their activity to managing their clients' assets without exercising any banking activity described above.

(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 persons from disclosing customer data entrusted to them or observed in their capacity as:

- A member of an executive or supervisory body.
- 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.)

A bank secrecy violation is punishable 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 banking secrecy violations when data is disclosed in Switzerland or abroad (Article 8(1), Swiss Criminal Code) (amended January 2017) (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, but not limited to:

- 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 the customer about his 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 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 (amended September 22, 2016). That Circular 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.)

The Banking Act only protects information related to an identified or identifiable customer. A bank can therefore disclose customer data by, for example, anonymizing the customer name, account number, online identifier, or other identifying information, or by aggregating customer data. 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 (Page 35, Annex 3, FINMA Circular 2008/21).

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, but are not limited to:

- **Governance risks.** Banks must systematically identify, mitigate, and monitor risks in connection with customer data. An independent unit must exercise control over the function of creating a security framework.
- **Data classification.** A bank 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 rights approvals and deletion and disposal of backup and operational systems.
- **Data localization.** A bank must maintain an inventory of:
  - where it stores 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 select, train, and monitor employees and third parties with access to customer data regularly (see Outsourcing Considerations). The bank is expected to maintain a list of all internal and external IT users that have access to mass customer data (key employees only).
- **Risk identification and control.** The 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 are expected to 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 exceptions allow a bank to disclose customer data protected by the banking secrecy obligation. Permissible disclosures include:

- Disclosure of customer data when requested under a Swiss statute requiring disclosure of information to a government authority (Article 47(5), Banking Act).
- Disclosure to a parent company that is supervised by a banking or financial market supervisory authority 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 financial intermediaries that are subject to a license;
  - the parent company and supervisory authority responsible for consolidated supervision are bound by official secrecy or professional confidentiality; 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.)

- Disclosure of customer data 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.)

- Disclosure to comply with a bank's reporting obligations under Swiss law including, for example, laws that require:
  - banks to provide FINMA with all information and documents that it requires to carry out its tasks including customer data (Article 29, Federal Act on the Swiss Financial Market Supervisory Authority (June 22, 2007)) (FINMASA));
  - banks to immediately report to FINMA any incident of substantial importance to the bank's supervision (Article 29, FINMASA); and
  - banks to report to the Money Laundering Reporting Office when it has knowledge or reasonable suspicion 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 (amended January 2016)).
- Disclosure of customer data to comply with agreements Switzerland has entered into with other countries including for example:
  - 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 countries signatories to the agreement to help fight tax evasion; and
  - the Agreement between the United States of America 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.

The exceptions permitting disclosure of customer data under the Banking Act are narrow and do not include many disclosures that banks typically need to make. 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 proceeding 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 the bank secrecy interests outweigh the interest in establishing the truth (Article 163(2) and Article 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 direting 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 as well as under 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 being investigated 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 specifically address the disclosure of customer data with 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 get customer consent at the account opening when the customer signs an application form with a clause incorporating the bank's standard terms and conditions. To ensure the customer understands the scope of disclosure, banks obtaining consent to disclose customer data 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 (W-008-8111).

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

The Federal Act on Data Protection (19 June 1992) (FADP) and the Ordinance to the Federal Act on Data Protection (14 June 1993) (Ordinance) apply to the processing of personal data pertaining to natural persons and legal persons (data subjects) by either:

- Natural or legal persons.
- Federal bodies.

(Article 2(1), FADP.)

CATEGORIES OF PERSONAL DATA

The FADP defines personal data as all information relating to an identified or identifiable natural or legal person (Article 3(a), FADP). Sensitive personal data is data relating to:

- Religious, ideological, political, or trade union-related views or activities.
- Health.
- Racial origin.
- Social security measures.
- Administrative or criminal proceedings and sanctions.

(Article 3(c), FADP.)

The FADP is currently under revision to adapt to developments in the EU, in particular the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and the Data Protection Convention of the Council of Europe (ETS 108). A draft version of the new Swiss data protection law was released on September 15, 2017 and the law is expected to come into force earliest in August 2018.

APPLICABILITY OF FADP

The FADP applies to any personal data processing that occurs within Switzerland (territoriality principle). In *Google Street View* (A-7040/2009), the Federal Administrative Court stated the FADP may further apply where a data processing operation is primarily connected with Switzerland, even if the personal data is saved on servers abroad (for example, through cloud computing) or published from abroad.

The FADP does not apply to certain types of data processing including, for example, data processing in the context of:

- Pending civil proceedings.
- Criminal proceedings.
- International mutual assistance proceedings.
- Proceedings under constitutional or under administrative law, except for first instance administrative proceedings (this means the lowest or first of several governmental authority proceedings).

(Article 2(2), FADP.)

Banks should review the FADP for exempt data processing activities to determine applicability.

PRINCIPLES

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

- Organizations must process personal data lawfully, in good faith, and proportionately, meaning the organization should limit the personal data processing to what is necessary for the organization to achieve the purpose of processing.
- Organizations 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 provides that:

- Anyone who processes personal data must ensure that it is correct (Article 5, FADP).
- Anyone who processes personal data must protect it against unauthorized processing through adequate technical and organizational measures (Article 7, FADP).
- Any person may request information from the organization responsible for personal data processing (data controller) about the personal data processing activities pertaining to that individual. The data controller must then notify the data subject about those 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 Consent Under the Data Protection Law).
- 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.

(Article 13(1), FADP.)

The FADP recognizes the overriding interest of the person processing the data if that person:

- Processes personal data in direct connection with the conclusion or the performance of a contract and the personal data is that of a contractual party.
- Is or intends to be in commercial competition with another and for this purpose processes personal data without disclosing the data to third parties.
- Processes data that is neither sensitive personal data nor a personality profile to verify the creditworthiness of another, and discloses that data to third parties only if the data is required for the conclusion or the performance of a contract with the affected individual or entity (data subject).
- Processes personal data on a professional basis exclusively for publication in the edited section of a periodically published medium.
- Processes personal data for purposes not relating to a specific person, in particular for the purposes of research, planning, and statistics and publishes the results in a manner that the data subjects may not be identified.
- Collects data on a person of public interest, provided the data relates to the public activities of that person.
- (Article 13(2), FADP.)
- Disclosure of personal data to third parties is generally lawful under the same conditions as outlined above. 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)

For more information on Switzerland's data protection rules and principles, see Country Q&A, Data protection in Switzerland: overview (9-502-5369).

DATA TRANSFER RESTRICTION

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 Swiss Federal Data Protection and Information Commissioner (FDPIC) has published a list of jurisdictions that it considers to provide adequate protection. In cases of transfers to the US, the data recipient can also receive personal data if it is certified under the Swiss-US Privacy Shield Framework.

For more information on certifying under the Swiss-US Privacy Shield Framework, see Privacy Shield Self-Certification Checklist (W-002-7961).

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

- The data subject consents to the transfer.
- The organization 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 a contractual party.
- 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 life or the physical integrity of the data subject.
- The data subject has made the personal data generally accessible and has not expressly prohibited its processing.

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

Organizations that use measures set out in the second bullet above to transfer personal data must inform the FDPIC of those measures (Article 6(3), FADP). However, if the organization transfers personal data based on FDPIC pre-approved safeguards (for example, model data transfer agreements issued by the FDPIC on its website found here), banks only need to inform the FDPIC that they are using these arrangements to transfer personal data (Article 6(3), Ordinance).

CONSENT UNDER THE DATA PROTECTION LAW

If an organization complies with the general data processing principles set out in the FADP (see Principles), the data subject does not need to consent to the personal data processing. 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).

The FADP provides that if an organization needs data subject consent to process personal data, the consent is valid only if the data subject:

- 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 that data subjects consent in writing. Therefore, consent given orally or via electronic means (for example, by mouse click) is generally deemed sufficient. However, the organization processing data 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).

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

CUSTOMER DATA COVERED BY THE FADP AND THE BANKING ACT

Banks in Switzerland handling customer personal data likely face compliance obligations under both the Banking Act and the FADP (see Data Protection Law) when collecting and processing customer personal data.

ANALYZING COVERED DATA

Organizations 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 and 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. In contrast, 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 personal data while the Banking Act protects the disclosure of covered customer data.

POTENTIAL CONFLICTS

The Banking Act and the FADP serve the same purpose of protecting data from access by unauthorized third parties. However, the Banking Act permits or requires banks to disclose data under certain circumstances (see Banking Act Exceptions Permitting Disclosure). In those circumstances, the FADP permits the processing and disclosure of personal data because the disclosure is authorized under another Swiss law. (Article 13(1), FADP.)

Banks may face a conflict between the Banking Act and the FADP where one law allows for disclosure of information and the other does not. For example, the FADP generally allows disclosure of customer personal data in accordance with the general principles (see Principles) while the Banking Act as a principle 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

BANKING ACT

Outsourcing 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 will then be considered bank representatives under Article 47 and functionally integrated into the bank's organization.

Banks may outsource services to third parties without FINMA approval if they comply with FINMA Circular 2008/7 and the FADP. However, the bank is responsible for customer data during the entire life cycle of the outsourced services and must take steps to protect customer data.

FINMA Circular 2008/7 sets out requirements for banks outsourcing services to third parties involving customer data or personal data under the FADP. Circular 2008/7 requirements include, but are not limited to, the following:

- Banks must make a Swiss outsourcing provider subject to the outsourcing institution's business secrecy rules. The Swiss service provider must explicitly commit to maintain the confidentiality of all customer personal data.
- Banks outsourcing to third-party service providers located outside of Switzerland must ensure that the third party has appropriate technical and organizational measures to comply with Swiss law's banking secrecy and data protection provisions.
- Organizations must inform banking customers of the outsourcing arrangement before they transmit customer data to the outsourcing provider in the:
  - bank's general terms and conditions;
  - safe custody regulations;
  - account statements;

  - informational brochures; or
  - by submitting information letters.
- The information must contain details on the specific business and service areas subject to the outsourcing initiative.
- Before organizations transfer bank customer data abroad for outsourcing purposes, they must inform customers by separate letter:
  - about the security measures the bank takes to protect customer data; and
  - that the customer has the opportunity to discontinue the contractual relationship within a reasonable timeframe and without suffering any disadvantages.
- The duty to provide this information does not apply if the data outsourced abroad does not directly or indirectly identify a customer.
- Banks must have the contractual right to audit the outsourced business at any time. When outsourcing abroad, the bank must demonstrate that its external auditor under bank and stock-exchange laws and the FINMA can assume and legally enforce their auditing rights.

FINMA Circular 2008/7 also requires banks to comply with detailed measures requiring the bank to:

- Carefully select, instruct, and control the outsourcing provider.
- Enter into a written contract with the outsourcing provider setting out, among other things, security requirements and the obligation to comply with bank secrecy rules.

Circular 2008/7 will be replaced by new Circular 2018/3 on April 1, 2018. The new Circular 2018/3 omits any references to data protection law and banking secrecy law. This means that FINMA no longer wants to make these particular areas the object of its regulation. However, banks outsourcing services will still need to fully comply with the FADP and the requirements in Annex 3 to FINMA Circular 2008/21 (see Principles for Managing Customer Data).

FADP

Under the FADP, the processing of personal data may be assigned 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 10(2), FADP.)

The bank continues to be 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. The third-party service provider must not use the data for its own purposes. If the provider is located outside of Switzerland, the bank must also comply with the FADP's cross-border transfer requirements (see Data Transfer Restriction).

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 3,000 Swiss Francs. 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 250,000 Swiss Francs (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.** According to Article 35 of the FADP, anyone who:
  - without authorization, willfully discloses confidential, sensitive personal data, or personality profiles received in the course of their professional activities is, on complaint, liable for a fine; and
  - the same penalties apply to anyone who without authorization 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.
- **Data subject lawsuits.** Data subjects can request that:
  - data processing be stopped;
  - that no data be disclosed to third parties; or
  - that the personal data be corrected or destroyed.

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

02-18