mandaris

Newsletter November 2025

THE SWISS ANTI-MONEY LAUNDERING ACT (AMLA) IN CONFLICT WITH THE SWISS DATA PROTECTION ACT (FADP)?

WHAT FINANCIAL INTERMEDIARIES NEED TO KEEP IN MIND

An issue not to be underestimated; since the entry into force of the revised FADP, natural persons (rather than the legal person acting) may be fined up to CHF 250,000 for violations of the FADP.

As the revised FADP has now been in force for more than two years. Now is an opportune time for financial intermediaries (FIs) to revisit and refresh themselves to the implications and requirements.

1. Present situation:

Under the AMLA, FIs are legally obliged to collect comprehensive personal data to identify the contracting party determine the beneficial owner(s) and details to transactions. In addition, there is an obligation for FIs to create a customer profile (KYC) and for high-risk business relationships (GMER) or high-risk transactions (TMER), FIs are subject to obtain substantial information to support or document adherence to the requirements.

Furthermore, there are comprehensive retention requirements stipulated under the AMLA. In practice, particularly in connection with international clients, domestic and foreign FIs, and in some cases tax authorities, require documented information that goes far beyond the prescribed statutory limitation and retention periods. Clients often expecting their FI to have retained such data, to be able to satisfy such request.

In contrast, the FI is confronted with the data processing principles of proportionality and transparency under the FADP. The former gives rise in particular to the obligation to minimize and to process data only to the extent necessary for the purpose of processing. Moreover, there is an obligation to delete data once its purpose has been fulfilled.

The tenor of the AMLA seems to be that the more data, the better which is conceptually at odds with the FADP. What does this mean in practice?

2. General relationship between the AMLA and the FADP:

In the event of violations of the data processing principles under the FADP, committed by the FIs in the application of the due diligence obligations under the AMLA, the FI may, if necessary, invoke the legal justification under Art. 31 para. 1 FADP. However, the FI cannot assume a fundamental derogation from the FADP in the application of the AMLA.

According to Art. 33 AMLA, the processing of personal data within the framework of the AMLA is generally governed by the FADP. Data processing in connection with reports of suspected money laundering pursuant to Art. 9 AMLA (or Art. 305 para. 2 of the Swiss Criminal Code (SCC)) is considered particularly sensitive by the legislator and is governed separately by Art. 34-35a AMLA.

3. Practical implementation:

FIs must comply with the data processing principles of the FADP, even when fulfilling their due diligence obligations under the AMLA. This applies in particular to:

- **Proportionality (Art. 6 para. 2 FADP):** Data processing must not go beyond what is necessary to fulfil the purpose of the processing. For example, databases (CRM, etc.) should have access restrictions. It would also be inadmissible to conduct a comprehensive, in-depth investigation into the origin of assets (source of funds, source of wealth) applied to every customer relationship without a corresponding reason under the AMLA (GMER, etc.).

- **Transparency requirement (Art. 6 para. 3 FADP):** When personal data is collected, the purpose of the collection must be clear to the data subject. In this context, the duty to provide information pursuant to Art. 19 FADP must be observed. In practice, controllers attempt to comply with this obligation by means of general data protection declarations via online privacy notices.

- **Purpose limitation (Art. 6 para. 3 FADP):** Personal data may only be processed to the extent that it is compatible with the purpose of collection e.g. data collected for the purpose of identifying the contractual partner may not be used per se for marketing purposes, such as newsletters, etc. Once the purpose has expired, the data must be deleted.

- **Data accuracy (Art. 6 para. 5 FADP):** The FI must ensure that the data processed is accurate and that it takes reasonable measures to ensure that data that is inaccurate or incomplete in relation to the purpose of its collection or processing is corrected. For example, changes of address or new telephone numbers of customers must be kept up-to-date, with FIs

periodically obtaining confirmations or seeking notifications to any such changes from its customers.

- **Data security (Art. 8 FADP):** The FI must ensure data security by taking appropriate technical and organizational measures. By way of example, appropriate technical (firewalls, encryption) and organisational (training, internal policies) measures are required.

4. Further obligations under the FADP:

In addition to the aforementioned data processing principles, the following is intended to illustrate the basic obligations of FIs under the FADP, including any sanctions in the event of a breach.

Record of processing activities

In fulfilling due diligence obligations under the FADP, FIs must also consider a possible obligation to create a record of processing activities (Art. 12 FADP) - this refers to an overview of all data processing within the company. In particular, it must contain information about the identity of the controller, the purpose of the processing and a description of the categories of data subjects and personal data processed, as well as the recipient of the data.

For small and medium-sized enterprises (SMEs), the Federal Council has provided for an exemption from the obligation to create a record of processing activities (Art. 12 para. 5 FADP). However, a look at the sanctions provisions of the FADP (Art. 60 ff. FADP) shows that failure to comply with this obligation does not result in any direct sanctions. For reasons of clarity, control and in view of potential requests for information from data subjects, it is nevertheless recommended for SMEs to keep a record of processing activities.

Data Protection Officer (DPO)

A DPO can advise and support management, mitigate risks and reduce misinterpretation or external consultation to the requirements arising from the FADP. In order to circumvent personal liability a DPO should only advise and not make decisions themselves. In contrast to the European General Data Protection Regulation (GDPR), the FADP does not require FIs to appoint a DPO.

Whilst the appointment of a DPO in a Swiss context does not bring any relevant (legal) advantage, it does circumvent the obligation to consult with the Federal Data Protection and Information Commissioner (FDPIC) in the context of a data protection impact assessment (Art. 23 para. 4 FADP).

Data protection impact assessment (DPIA)

Pursuant to Art. 22 FADP, FIs must always consider a data protection impact assessment in accordance with Art. 22 FADP if data processing may pose a high risk to the personality or fundamental rights of the data subject. This applies in particular to AI-supported applications for processing personal data. The purpose of the data

protection impact assessment is, on the one hand, to identify and assess risks and, on the other hand, to identify mitigating measures.

Private controllers, such as FIs are exempt from undertaking an assessment when processing is legally obliged, including when processed within the scope of the AMLA. Failure to perform a DPIA is not directly sanctioned under the FADP (see Art. 60 ff. FADP).

Cross-border disclosure of personal data

FIs must be aware of the requirements relating to the cross-border disclosure of personal data (Art. 16 ff. FADP). Data may only be transferred abroad if the foreign legislation offers adequate protection or corresponds to the Swiss level of data protection.

The Federal Council determines and publishes countries of equivalency in Annex 1 of the Data Protection Ordinance (DPOrd). If an FI wishes to transfer data to a country not listed in the DPOrd (in particular countries outside the European Economic Area (EEA)) it must namely rely on the below measures, as outlined within Art. 16 para. 2 lit. a-e FADP:

- international law treaties;
- corresponding data protection clauses in a contract
- standard contractual clauses (SCC); or
- binding corporate rules (BCR).

Art. 17 FADP permits exceptions to the provisions of Art. 16 FADP, including data subject consent or if disclosure is necessary to the conclusion or performance of a contract. Non-compliance may be subject to penalties under Art. 61 FADP.

Data breaches

Pursuant to Art. 24 FADP, data breaches that are likely to result in a high risk to the personality or fundamental rights of the data subject must be reported to the FDPIC. Additionally, FIs must also comply with regulatory reporting requirements, (in particular FINMA). Unlike to the GDPR, failure to report does not trigger direct sanctions under the FADP (see Art. 60 ff. FADP).

Controller and Processor of Data

When it comes to the processing of data involving third parties, the FI must be aware of the distinction between the roles of the controller and the processor:

- The controller decides on the purpose and means of data processing and therefore must determine why and how data is processed, and also bears the main responsibility for the lawfulness of the processing.
- The processor (e.g. a cloud provider), on the other hand, never processes personal data for its own purposes, but exclusively on behalf of and on the instructions of the controller.

The controller must ensure that the cooperation with the processor is contractually regulated and complies with the requirements of the FADP.

Right to information

According to Art. 60 FADP, failure to comply with information obligations towards data subjects when obtaining personal data, or upholding the right of data subjects rights of request, may be subject to fines. The same applies to anyone violating its obligations to cooperate in investigations by the FDPIC.

5. Conclusion:

FIs are ever increasingly operating within the intersection of regulatory regimes, often with fundamentally opposing approaches. AMLA requiring a broad, risk-based collection of data, while the FADP demands a narrower scope, transparency and deletion.

Should you need support in implementing a compliant process and framework to the above or have any questions on the topic, do not hesitate to contact us.

The Author:

Dominik Wasmer
MLaw (University of Basel), TEP, DAS Compliance Management (HSLU)
CAS Data Protection (University of Zurich)

Vice President, Legal & Compliance Officer
dominik.wasmer@mandaris.com
Telephone: +41 61 285 17 17

Our locations:
Mandaris AG
St. Alban-Anlage 46
CH-4052 Basel
Tel. +41 61 285 17 17

Mandaris AG
Selnaustrasse 3
CH-8001 Zurich
Tel.

Mandaris AG
Chamerstrasse 174
CH-6300 Zug
Tel.

Mandaris Group (Malta) Ltd.
Forni Complex 1E, Level 2,
Pinto Wharf,
Valletta Waterfront
Floriana, FRN 1913
Malta
Tel.