Anti-money laundering and counter-terrorism financing policy

December 2022

Introduction

Background and purpose

The purpose of the policy is to ensure that the companies in the Group share the same compliance guidelines and procedures and that they work effectively and with a risk-based approach to prevent the company from being exploited for money laundering and terrorism financing purposes. This also contributes to sound business and good customer protection while reducing the risk that Avanza's brand will be adversely affected.

Scope and entry into force

This policy covers Avanza Bank AB, Avanza Fonder AB and Försäkringsaktiebolaget Avanza Pension ("the Companies") and comprises all employees, contractors and others who for similar reasons participate in the activities of the Companies.

The policy is effective as of the date it is approved by the Board of Directors of Avanza Bank Holding AB (publ).

Communication and introduction

The CEO of the Company shall inform every employee in a management position of the provisions of this policy and is responsible for its adoption.

Definitions

Money laundering refers to measures with respect to money or other property generated from criminal acts that:

- can disguise the connection between the property and the criminal act,
- can enable the persons involved to avail themselves of the property or its value,
- can enable the persons involved to circumvent legal consequences, or
- someone acquires, holds, claims right to or utilises the property.

Measures that typically are intended to disguise that a person intends to enrich themselves or others through future criminal acts are also covered by the term.

Terrorism financing refers to collecting, providing or receiving money or other property so that the property can be used, or in the knowledge that it is intended to be used, to commit a crime as referred to in the Anti-Terrorism Act.

Internal control

The Board of Directors and the CEO are ultimately responsible for ensuring that the necessary measures are taken to combat money laundering and terrorism financing, that internal rules meet external laws and regulations, and that these rules are appropriate, implemented and complied with.

Avanza will, for its anti-money laundering and counter-terrorism financing organisation, assess whether the Companies should name a specially appointed executive (SAE). If it is decided not to name a specially appointed executive, a detailed explanation is produced and documented. The decision is re-evaluated annually or if the business changes.

The Board of Directors delegates the specially appointed executive or, if the Company does not have an SAE, the Company's CEO responsibility for conducting and updating a general risk assessment of how the Company's products and services can be exploited for money laundering or terrorism financing and how big the risk is that this could occur, preparation and updating of policy documents, and that the Companies in general implement the measures and controls (first line) shown in this policy.

The Board of Directors appoints an officer for controlling and reporting obligations.

An independent audit function is included in Internal Audit.

Common principles for overarching risk assessments

Each Company shall have a process to establish its own general risk assessment of the risk that the Company will be exposed to money laundering and terrorism financing. Procedures shall be in place to execute, evaluate and update the general risk assessment.

The general risk assessment shall be designed to serve as the basis for the Company's procedures, guidelines and other measures to combat anti-money laundering and counter-terrorism. The general risk assessment shall be documented and kept updated.

The Company's SAE or, in cases where the Company does not have an SAE, the Company's CEO is responsible for ensuring that a general risk assessment is performed at least once a year or if the business changes.

General risk assessment

Each Company shall determine how the products and services it supplies can be exploited for money laundering or terrorism financing purposes and how large the risk is that this will occur (general risk assessment).

In the general risk assessment, special attention is given to the types of products and services which are provided, which customers and distribution channels exist and which geographical risk factors arise. Consideration is also given to information obtained from the Company's reporting of suspected activities and transactions as well as to information on the approach to money laundering and terrorism financing and other relevant information provided by authorities.

Risk assessment of customers

Each Company shall determine the risk of money laundering and terrorism financing associated with the customer relationship (the customer's risk profile).

The customer's risk profile will be determined on the basis of the general risk assessment and the Company's knowledge of the customer. The customer's risk profile is monitored and changed as needed.

Risk management

The risks that the Companies have identified in the general risk assessment shall be managed and serve as a basis for decisions how resources are allocated and which measures will be taken to reduce the risk of being exploited for money laundering and terrorism financing.

Reporting, documentation and updates

Each Company shall at least once a year inform the Company's board of directors of the risks of being exploited for money laundering and terrorism financing which have been identified and which measures have been taken to reduce the risks.

The general risk assessment shall be documented. The same applies to important underlying material used in the assessment.

The Companies' general risk assessment shall regularly, at least once a year, be evaluated and updated as needed. The Company shall update its risk assessment when events occur which can affect the risk in the Company's operations. For example, when the Companies offer new or materially altered products or services, target new markets, use new technology or make other material changes to its operations. These risks shall be identified in the Companies' NPAP process, after which their risk assessment is updated. New methods of money laundering and terrorism financing, new laws etc. may necessitate an update of the Companies' risk assessment.

Common principles for developing internal procedures

Each Company shall set out internal procedures to meet the requirements in the Anti-Money Laundering Act and regulations. These procedures shall be adapted to the risks identified in the general risk assessment and the Company's operations otherwise.

Each Company's CEO or board of directors shall annually set out guidelines that complement this policy. The procedures and guidelines shall be continuously adapted based on new and changing risks of money laundering and terrorism financing.

The scope and content of the procedures and guidelines shall be determined given the size, nature and risks of money laundering and terrorism financing which have been identified in the general risk assessment.

The guidelines will comprise:

- Procedures to implement, evaluate and follow up the general risk assessment with delegated responsibility for the various parts of the risk assessment process
- Procedures for the Know-Your-Customer (KYC) process
- Procedures for risk assessment of customers
- Procedures and systems to continuously monitor business relationships
- Procedures for retaining documents or actions which have been taken for KYC purposes
- Procedures and systems to monitor unusual transactions and activities as well as transactions and activities that while not unusual can be assumed to be part of money laundering or terrorism financing
- Procedures for reporting to the Swedish Police
- Procedures for retaining information gathered in reviews of suspected transactions
- Procedures for training employees on money laundering and terrorism financing issues
- Procedures for suitability assessments of employees
- Procedures to protect employees from threats, revenge or other hostile actions and reprisals
- Guidelines for internal control, compliance and internal information (on measures to combat money laundering and terrorism financing) to ensure that internal rules meet the requirements in applicable

laws and regulations and that an effective information and communication system is in place to ensure that the right knowledge is spread within the Company.
- For cases where the Companies use models for risk assessment, risk classification, oversight or other procedures, the Companies will have procedures for model risk management. The purpose of these procedures is to evaluate and quality assure the models that the Companies use.

Each Company shall maintain an appropriate reporting system for employees and contractors that want to report suspected non-compliance with the provisions of the Anti-Money Laundering Act or regulations – a whistleblower system.

Common procedures

The common procedures and the guidelines will comprise at a minimum procedures and guidelines for processing personal data and sharing information within the Group with respect to suspected money laundering and terrorism financing as well as other relevant information.

Processing of personal data

Each Company has previously established on a separate Group-wide policy and instruction on processing of personal data.

Information sharing within the Group

The purpose of the Anti-Money Laundering Act and the regulations is to prevent money laundering and terrorism financing. The information that can be shared must be important to the Companies and their ability to detect, mitigate and prevent money laundering and terrorism financing. According to the Anti-Money Laundering Act, information on suspected money laundering and terrorism financing can be shared with affected Companies.

Information that is shared

If, after review, suspicion still remains that an activity or transaction may involve money laundering or terrorism financing, it must be reported to the Financial Intelligence Unit within the Swedish Police.

Information on a natural or legal person that has been reported to the Financial Intelligence Unit shall be shared by the Companies. The information shall include which natural or legal person has been reported and the Company that reported it.

Complementary information

In certain cases, the Company may need to know why a natural or legal person has been reported to use it in a risk assessment of an existing customer, to compile information on a suspected transaction or activity for the Financial Intelligence Unit or to take a position whether a natural or legal person that has been reported by a Company may still establish a customer relationship with another Company.

Information on reported natural and legal persons is subject to the laws on bank secrecy. According to the Anti-Money Laundering Act, the companies within a group do not violate these bank secrecy laws when they share information on reporting. The information may not be disclosed more than necessary. If a Company needs complementary information on a report and its content, only a limited number of persons may request it.

Retention of information

The Companies' procedures for retaining information on actions or measures which have been taken to review unusual or suspected activities or transactions follow the regulations in effect at the time.

When the underlying documentation for a report is retained according to current regulations, information on whether a person has been reported may no longer be shared by the Companies.

Compliance

The CEO and every employee in a management position is responsible for complying with this policy document. The CEO is ultimately responsible for ensuring that the Company has self-assessments and procedures that guarantee good internal control. Employees, contractors and others that for similar reasons participate in the business and perform tasks of importance to preventing money laundering or terrorism financing shall be made aware of the content of the policy and comply with it.