

Policy for measures against money laundering and terrorist financing

20 June 2017

Contents

1. Introduction.....	3
2. AML Executive and AML Officer.....	3
3. Measures.....	3
3.1 Risk management.....	3
3.2 Organisation, resources and business procedures	4
3.3 Training	4
3.4 Customers	4
3.5 Politically exposed persons (PEPs).....	5
3.6 Correspondent banks and SWIFT keys	5
3.7 Monitoring.....	6
3.8 Reporting.....	6
4 Internal controls.....	6
5 Internal reporting.....	6

1. Introduction

The object of this policy is to determine the general guidelines for Sydbank's measures to prevent the Bank from being used for money laundering and terrorist financing.

This policy applies to the entire Sydbank Group, including all of the Bank's domestic and foreign activities.

It is the Bank's policy to comply with legislation and rules on money laundering and terrorist financing. To the extent that the Bank's activities are subject to foreign rules on money laundering and terrorist financing, such rules must moreover be observed.

2. AML Executive and AML Officer

The Bank has appointed an AML Executive from the Bank's Group Executive Management. The AML Executive must ensure that the Bank complies with legislation and rules governing money laundering and terrorist financing and that measures contained in this policy are implemented.

An AML Officer reporting to the Compliance Officer has been appointed. The AML Officer must support the AML Executive as well as approve business procedures, controls and procedures implemented pursuant to the Danish Consolidated Act on Measures to Prevent Money Laundering and Financing of Terrorism. Moreover the AML Officer must approve customer relationships with politically exposed persons (PEPs) and correspondent banks. The AML Officer may delegate tasks to named individuals.

3. Measures

The following measures must be implemented to prevent Sydbank from being used for money laundering and terrorist financing:

3.1 Risk management

An analysis must be prepared containing an assessment of the extent to which the Bank's business model and business volume are at risk of being used for the purpose of money laundering or terrorist financing. This money laundering risk analysis must be updated as appropriate and as a minimum once a year.

On the basis of the analysis the Bank must put into practice appropriate measures to mitigate the risk of the Bank being used for the purpose of money laundering and terrorist financing.

3.2 Organisation, resources and business procedures

The Bank must have an efficient organisation in place with a clear allocation of tasks related to anti-money laundering. Adequate resources must be available to ensure that the Bank complies with legislation governing money laundering and the measures specified in this policy.

An AML Committee has been established to assist in identifying and assessing the risk of the Bank being used for the purpose of money laundering and terrorist financing. Moreover the committee discusses and assesses the measures implemented by the Bank to counter money laundering and terrorist financing. The committee is attended by the group executive vice presidents of the business lines that have tasks relating to the Danish Anti-Money Laundering Act. The committee meets at least once every quarter.

In each of the Bank's business units within Retail Clients & Private Banking an employee has been appointed to act as an AML knowledge person. The employee must assist in the implementation of new measures against money laundering and terrorist financing as well as act as a sounding board in the discussion of problems related to the Danish Anti-Money Laundering Act.

Business procedures that clearly describe the measures to be carried out to mitigate the risk of the Bank being used for money laundering and terrorist financing must be made available to all relevant employees.

3.3 Training

The Bank's relevant employees must receive training in anti-money laundering rules at regular intervals and as a minimum once a year. The training must ensure that the Bank's employees are aware of their individual obligations in connection with carrying out their jobs. The Bank must be able to document which employees have received training.

3.4 Customers

New customers of the Bank must be identified and proof of their identity must be provided. The purpose of the business relationship as well as the expected scope

must be established. This applies to occasional as well as regular customer relationships. Where a customer is a legal person, the ownership and control structure must be clarified and the beneficial owners must be identified and proof of their identity must be provided.

The investigation of customers and the updating of information are carried out using a risk-based approach and on the basis of the assessed risks of the individual customer segments in the Bank's money laundering risk analysis. The Bank divides its customers into categories depending on whether the risk of money laundering or terrorist financing is low, moderate, elevated or high.

As a rule the Bank will not enter into or maintain customer relationships with customers who are resident in countries where there is a particularly high risk of money laundering or terrorist financing according to the assessment of the Danish Financial Supervisory Authority, the EU or FATF.

As a rule the Bank will not enter into or maintain customer relationships with customers who carry out activities connected with a particularly high risk of money laundering or terrorist financing according to the assessment of the Bank, the Danish Financial Supervisory Authority, the EU or FATF.

3.5 Politically exposed persons (PEPs)

The Bank must be able to identify and monitor customers who are PEPs on an ongoing basis and have a procedure in place for the approval of customers who are PEPs.

3.6 Correspondent banks and SWIFT keys

Cooperation with other banks is subject to a due diligence of the correspondent bank's compliance with anti-money laundering legislation. The implemented due diligence is updated regularly on the basis of a risk-based approach.

Sydbank will not maintain correspondent bank relationships or SWIFT keys with financial institutions that are resident in countries where there is a particularly high risk of money laundering or terrorist financing according to the assessment of the Danish Financial Supervisory Authority, the EU or FATF.

Sydbank has no business relationships with banks that have no physical presence (shell banks).

3.7 Monitoring

The Bank must be vigilant and monitor whether transactions conducted at Sydbank could be suspected of being related to money laundering or terrorist financing. Monitoring must be carried out both manually and by means of electronic systems.

As a part of the Bank's monitoring procedure, screening of customers and transactions against the EU's and the FATF's terrorist lists and other sanctions lists must be carried out on an ongoing basis.

3.8 Reporting

When the Bank's monitoring or other circumstances give rise to suspicions of criminal activities covered by the reporting requirement stipulated in anti-money laundering legislation, such activities must be investigated further. The investigation comprises eg specific information regarding a given transaction and the Bank's knowledge of the customer's circumstances. If as a result of the investigation the Bank is not able to immediately refute the suspicion, the Bank will file a report with the competent authorities. In some cases the Bank is obliged by law to freeze a customer's funds. The freezing of funds will be implemented and sustained in cooperation with the relevant authorities.

4 Internal controls

Regular internal controls must be implemented to ensure that the measures specified in this policy are carried out and are effective.

5 Internal reporting

The AML Officer must submit a report to the Bank's Executive Group Management and Board of Directors four times a year on the Bank's risks, measures implemented and internal controls regarding money laundering.