

Policy for prevention of money laundering, terrorist financing and sanctions breaches

Most recently updated on 26 March 2019

26 March 2019

Contents

1. Purpose.....	3
2. Organisation and governance	4
3. Risk assessment	5
4. Measures.....	5
4.1 Customers	5
4.2 Customer due diligence procedure.....	6
4.3 Screening of customer database and foreign transactions	6
4.4 Transaction monitoring.....	7
4.5 The Bank’s employees.....	7
5. Risk management.....	8
6. Collection and storage of data	8
7. Approval and update of the Policy	9

1. Purpose

The purpose of this Policy is to establish the general guidelines for Sydbank's measures to prevent the Bank from being used for money laundering, terrorist financing and sanctions breaches. Moreover the Policy must ensure that Sydbank complies with the rules of the Danish Consolidated Act on Measures to Prevent Money Laundering and Financing of Terrorism (the Danish Money Laundering Act) as well as existing national and international sanctions provisions. As regards the Bank's branches in Germany, Sydbank must furthermore comply with relevant legislation in Germany if such legislation contains more stringent requirements than Danish legislation.

The guidelines set out in this Policy constitute the Board of Directors' instructions to the Group Executive Management.

The Danish Money Laundering Act defines money laundering as follows:

1. To unlawfully receive or obtain for oneself or others a share in economic profits or funds obtained through a criminal offence.
2. To unlawfully conceal, store, transport, assist in the disposal of or otherwise subsequently serve to ensure the economic profits or funds obtained through a criminal offence.
3. Attempt at or participation in such actions.

The Danish Criminal Code defines terrorist financing as any person who:

- directly or indirectly grants financial support to
- directly or indirectly provides or collects funds for, or
- directly or indirectly makes money, other financial assets or financial or other similar services available to

a person, a group of persons or an association that commits or intends to commit acts falling within the scope of Section 114 or 114a (terrorist acts).

Sanctions are restrictions passed by the UN, EU and OFAC against certain countries and/or persons, legal entities, bodies etc.

This Policy applies to the entire Sydbank Group and its employees, including the Bank's branches in Germany.

An appendix to this Policy has been drafted detailing the framework for Sydbank's risk tolerance in relation to the Danish Money Laundering Act and the sanctions rules. The appendix constitutes part of the Policy but can only be accessed internally in the Bank.

2. Organisation and governance

Sydbank has appointed an AML Executive from the Bank's Group Executive Management. The AML Executive must ensure that Sydbank implements this Policy and complies with applicable legislation and rules concerning money laundering, terrorist financing and sanctions.

Moreover Sydbank has appointed an AML Officer who is tasked with the ongoing monitoring of Sydbank's risk of money laundering and terrorist financing and with making decisions affecting risk exposure including approving the policies, controls and procedures in place to limit the Bank's risk of being used for money laundering and terrorist financing. Furthermore the AML Officer must approve business relationships with politically exposed persons and correspondent banks before establishing customer relationships as well as at regular intervals during such customer relationships.

The AML Officer reports to the Group Executive Management on a quarterly basis and alternately to the Board of Directors and its Risk Committee 4 times a year. Moreover the AML Officer must report on an ad hoc basis to the AML Executive when deemed necessary.

Furthermore an AML Committee has been established to assist in identifying and assessing the risk of the Bank being used for money laundering and terrorist financing. Moreover the AML Committee discusses and assesses the measures implemented by the Bank as regards money laundering, terrorist financing and sanctions. The committee is attended by the group executive vice presidents (or representatives appointed by them) of the divisions that have tasks relating to the Danish Money Laundering Act and the sanctions rules. The AML Executive is the chairman of the committee, which meets at least once every quarter.

The business units together with the quality assurance department have the principal responsibility for establishing, complying with and overseeing the measures implemented to minimise money laundering and terrorist financing (first line of defence).

The Compliance Officer must oversee and assess whether the Bank's measures in relation to money laundering are efficient (second line of defence) and the Bank's Internal Audit Department must oversee whether the measures are organised and function satisfactorily (third line of defence).

3. Risk assessment

Sydbank has prepared a risk assessment in which the risk of the Bank being used for money laundering and terrorist financing is identified and assessed.

The conclusions of the risk assessment form the basis of the policies, procedures and controls that Sydbank must implement to prevent, limit and manage the risks identified.

The risk assessment is updated on an ongoing basis when significant changes are made to the Bank's business model or when new risks are identified – however at least once a year. In connection with the update, the risk assessment must be presented to the AML Committee for comments before being approved by the Group Executive Management and presented to the Board of Directors for information purposes.

4. Measures

4.1 Customers

As a nationwide bank, Sydbank has a significant presence in all parts of Denmark as well as in Northern Germany. The Bank's customers must have a natural connection to the Bank's area of operation, meaning that the customer must have a geographical or a commercial connection to Denmark or Northern Germany. Sydbank will not enter into and maintain customer relationships where the Bank:

- cannot complete a full customer due diligence procedure
- cannot comprehend the customer's business model
- cannot obtain a comprehensive view of the origin of the customer's assets and funds.

Neither does Sydbank wish to enter into or maintain customer relationships with persons suspected of having committed financial crimes, money laundering, terrorist acts or appearing on an official sanctions list.

Cooperation with other banks is subject among other things to a due diligence of the correspondent bank's compliance with anti-money laundering legislation. Sydbank will not establish business relationships with banks that have no physical presence (shell banks).

For further specification of the Bank's risk tolerance as regards money laundering, reference is made to "Risikotolerance – Hvidvaskloven" ("Risk tolerance – Money Laundering Act") (internal document).

In compliance with the provisions of the Danish Money Laundering Act, Sydbank has chosen a risk-based approach to areas in which the Bank may be used for money laundering and terrorist financing. This means that the Bank allocates most resources to the areas and the customers considered to pose the greatest risk for the Bank in terms of money laundering and terrorist financing.

4.2 Customer due diligence procedure

A customer due diligence must be carried out for all the Bank's customers:

- when a customer relationship is established
- when single transactions are executed on behalf of occasional customers
- when changes are made to the customer relationship
- at appropriate intervals during the customer relationship based on the customer's risk profile (low, moderate, medium-high or high).

In case of new as well as existing customer relationships the Bank must:

- verify and oversee the identity of the customer and the beneficial owners, if any. Sydbank requires the customer to produce valid identification documents.
- be able to obtain a comprehensive view of the customer's business model and group structure.
- ensure that it has adequate information about the purpose and intended nature of the customer relationship.
- have a complete knowledge of the customer's ownership structure including the beneficial owners.

The amount and degree of the information and documentation to be obtained depend on the customer's risk profile, which is determined according to internal guidelines.

4.3 Screening of customer database and foreign transactions

Sydbank must have efficient systems for screening the customer database at regular intervals against:

- official UN, EU and OFAC sanctions lists

- Danish and foreign lists of politically exposed persons.

In addition the Bank must have efficient systems and procedures for scanning transactions against official UN, EU and OFAC sanctions lists.

If the screening shows an identity match, the Bank must immediately freeze the customer's funds. The freezing of funds will be made and sustained in cooperation with the relevant authorities.

4.4 Transaction monitoring

Sydbank must have efficient transaction monitoring combined with the account manager's due diligence ensuring that suspicious transactions and activities are investigated further.

The monitoring must focus on whether the customer's transactions and activities are consistent with the stated purpose of the customer relationship and the expected scope as well as whether the customer's transactions in other respects differ from those of similar customers. The transaction monitoring serves as a basis for assessing whether there are grounds to suspect money laundering and terrorist financing.

When the Bank's monitoring or other circumstances give rise to suspicions of or reasonable grounds to suspect criminal activities covered by the reporting requirement stipulated in anti-money laundering legislation, such activities must be investigated further. All investigations must be documented. The documentation must include sufficient information about the facts of the case, the assessment and the outcome of the investigation. 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 Danish Money Laundering Secretariat. The Bank's employees are under a duty of non-disclosure in the event that a report has been filed in accordance with the Danish Money Laundering Act.

4.5 The Bank's employees

The Bank's employees must have access to business procedures and other internal guidelines establishing the framework for how the Bank guards against being used for money laundering and terrorist financing.

The internal guidelines must be operational so that individual employees have a clear understanding of their obligations and responsibilities. A central unit at the Bank's

head office ensures that the internal guidelines are accessible, understandable, updated and approved by the AML Officer.

Employees charged with tasks related to anti-money laundering legislation must receive training at regular intervals in applicable rules relating to anti-money laundering, terrorist financing and sanctions as well as Sydbank's internal guidelines. The training must ensure that the Bank's employees understand risks and 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.

The Bank's employees are screened against available sanctions lists on equal terms with the Bank's customers to ensure that the Bank's staff are not associated with terrorist groups subject to sanctions by the authorities. Moreover all employees must at any time be able to produce a criminal record certificate which does not give rise to comments in respect of financial crime or similar with significance for their work related to anti-money laundering legislation.

5. Risk management

To ensure good risk management relative to the Bank's risk of being used for money laundering and terrorist financing, internal controls must be performed on an ongoing basis by the first line of defence to establish whether the Bank has sufficient measures in the relevant area and whether such measures are effective.

The AML Officer reports quarterly on the results of these controls as well as the benchmarks set out in the appendix to this Policy ("Risikotolerance – Hvidvaskloven og sanktionsregler" ("Risk tolerance – Money Laundering Act and sanctions rules")) to the Group Executive Management and Board of Directors, who decide on an ongoing basis whether the results of the controls and benchmarks are acceptable relative to the Bank's risk tolerance.

6. Collection and storage of data

Sydbank collects the information and documents necessary to perform the duties imposed on the Bank in accordance with the Danish Money Laundering Act and ancillary provisions and instructions.

The information and documents collected and the relevant registrations must be stored in such a manner that only relevant employees have knowledge of the material collected.

The Bank stores the information electronically under the unique reference number(s) of the customer and the beneficial owner. The information, documents and registrations are stored for at least 5 years after termination of the business relationship.

Information, documents and registrations collected are passed on to the State Prosecutor for Serious Economic and International Crime as stipulated in the Danish Money Laundering Act or related legislation.

Moreover information is passed on internally in the Bank where this is deemed necessary owing to the obligations imposed on the Bank in accordance with the Danish Money Laundering Act. For instance there must be an exchange of information between the Danish and German branches when suspicious transactions or activities are observed which must be investigated further and which may result in the Bank notifying the authorities.

Reference is made to Sydbank's policy for the processing of personal data.

7. Approval and update of the Policy

The AML Officer is responsible for ensuring on an ongoing basis that necessary updates of this Policy are presented to the Board of Directors. As a minimum the Policy must be updated annually when Sydbank's risk assessment has been updated and approved by the Group Executive Management.

Sydbank's Board of Directors approves this Policy and the appendix "Risikotolerance – Hvidvaskloven og sanktionsregler" ("Risk tolerance – Money Laundering Act and sanctions rules"). Following the approval the Policy is made available on the Bank's website in Danish and English and on the Bank's intranet. The appendix is only available on the Bank's intranet.