Sydbank

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

17 December 2020

Document no 8m

Contents

1. Purpose

The purpose of this Policy is to establish the general guidelines for Sydbank's measures to prevent financial crime and 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.

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.

The guidelines set out in this Policy constitute the Board of Directors' instruction to the Group Executive Management and apply to Sydbank in its entirety and all employees – including Sydbank in Germany.

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).

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

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. Governance – tone from the top

To ensure the necessary focus on combating money laundering and terrorist financing, the tone from the top must be clear so that all the Bank's employees understand the importance of their responsibility and tasks in relation to the obligations under the Danish Money Laundering Act.

In this connection Sydbank has appointed an AML Executive (Group Executive Management member). In addition to ensuring the implementation of this Policy and compliance with existing legislation, the AML Executive must help to ensure that the rest of the management at the Bank focuses on this area so that tasks are duly performed by employees.

The AML Executive is the chairperson of the Bank's AML Committee. The AML Committee discusses the Bank's efforts to combat money laundering and terrorist financing and consists of group executive vice presidents (or representatives appointed by them) of the divisions with tasks within this area. The discussions on strategy and the progress regarding combating money laundering and terrorist financing are to ensure uniformity and focus in the Bank's central as well as decentralised business units. The AML Committee meets at least once every quarter.

The AML Risk Management department, which is headed by the risk officer as regards AML, reports on a regular basis to the AML Executive and the AML Committee when new risks are identified at the Bank and on the overall progress in this area at the Bank as well as in society. This ensures that the top management at the Bank can give the necessary instructions to the Bank's employees. Risks concerning the Bank's German branches are identified and reported to AML Risk Management by the AML officer at Sydbank in Germany.

3. Risk management

To ensure efficient measures to prevent criminals from using Sydbank for money laundering and terrorist financing, it is important that the Bank's risk management in this area is robust. At Sydbank risk management must consist of the following elements:

Risk assessment

On the basis of the Bank's business model AML Risk Management conducts an assessment of the business units where there is a risk that the Bank may be used for

money laundering and terrorist financing. The assessment takes into consideration the inherent risk as well as the estimated remaining risk when the Bank's measures in this area have been accounted for. The AML officer at Sydbank in Germany prepares an assessment of the German branches that takes into account any special circumstances applying there.

The risk assessment is updated on an ongoing basis when significant changes are made to the Bank's business model – however at least once a year. In connection with the updating 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.

When new risks are identified that do not give rise to an updating of the risk assessment, they must be brought before the AML Committee. Previously identified risks that are no longer relevant must also be brought before the AML Committee before being deleted from the risk assessment.

Policy and business procedures

The AML Policy, business procedures and job descriptions giving the Bank's employees instructions on how to handle identified risks are formulated on the basis of the risks described in the risk assessment.

The Quality Assurance – AML & GDPR department is responsible for formulating and updating the Bank's business procedures in this area as well as ensuring that appropriate tools and processes are made available to employees so that they are in no doubt as to their duties and responsibility and are thereby able to carry out the necessary tasks in an appropriate manner. The AML officer at Sydbank in Germany formulates business procedures for the German branches in areas where conditions differ from those in Denmark.

The AML Policy is formulated by AML Risk Management and approved by the Bank's Board of Directors. Business procedures regarding combating money laundering and terrorist financing must be approved by AML Risk Management. This also applies to special business procedures formulated for the branches in Germany.

Controls

To ensure compliance with business procedures a number of controls of work performed by employees are carried out. The controls are implemented partly by the individual business units, partly by central control units as well as by AML Risk Management. AML Risk Management must approve the implementation of new controls and has the overall responsibility for ensuring that the Bank has appropriate controls covering the identified risks in this area.

The AML officer at Sydbank in Germany conducts controls regarding the German branches if they are not included in the controls performed by the head office.

Three lines of defence

The business units together with Quality Assurance – AML & GDPR 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).

Reporting

The head of AML Risk Management reports to the AML Committee and the Group Executive Management on a quarterly basis. In addition the head of AML Risk Management reports alternately to the Board of Directors and its Risk Committee 4 times a year. Moreover ad hoc reporting to the AML Executive (Group Executive Management member) occurs when deemed necessary. The AML officer at Sydbank in Germany reports on a quarterly basis to the Group Executive Vice President of Sydbank in Germany and to AML Risk Management, which ensures that the status report of the German branches is included in the report from AML Risk Management.

The quarterly reporting must include a general progress report of the Bank's efforts to combat money laundering and terrorist financing – however as a minimum a status report regarding:

- the Bank's controls – permanent as well as ad hoc
- the Bank's transaction monitoring
- new risks and legislation, if any
- Sydbank in Germany
- current reports from Compliance, Internal Audit and the Danish FSA
- compliance with the risk tolerance determined by the Bank in this area.

4. Measures

4.1 Customers

A KYC procedure must be carried out for all the Bank's customers when a customer relationship is established as well as at regular intervals during the customer relationship. The content and the scope of the KYC procedure appear from the Danish Money Laundering Act and are specified in the Bank's business procedures. Furthermore all customers must have a risk profile establishing the framework for the KYC procedure. AML Risk Management determines the parameters for creating risk profiles. Any changes and adjustments made by AML Risk Management must be reported to the AML Committee.

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.

As part of the Bank's efforts to reduce the risk of being used for money laundering and terrorist financing, there are customers and types of customers with whom Sydbank does not wish to establish a customer relationship unless required to do so by other legislation:

1. Customers who do not wish to provide adequate and sufficient information in connection with the KYC procedure.
2. Customers who are unable to account for the origin of their assets and funds.
3. Businesses and associations whose business model/articles of association/bylaws give(s) rise to doubt that the activity of the business or association is legal.
4. Businesses with a group structure that is not transparent and/or does not make sense with regard to the business model of the business in question.
5. Partial customers who only wish to use Sydbank as a financial conduit or for their cash transactions.
6. Offshore companies (a company established in a country that does not have a natural connection to the operations of the company or the beneficial owner). Examples of "offshore" are Belize, Vanuatu, the Bahamas and the Cayman Islands.
7. Trusts and similar legal arrangements domiciled outside Denmark and Germany.
8. Associations that are not formally established with bylaws, a general meeting and a supervisory board.
9. Banks with no physical presence (empty companies/shell banks).
10. Foreign exchange bureaus.
11. Businesses that offer, trade or store cryptocurrencies.
12. Cash-based gambling.
13. Businesses offering consumer loans.
14. Money transfer businesses.

The establishment of customer relationships with the following persons or businesses is subject to approval by AML Risk Management or the division to which AML Risk Management has delegated the task of approval:

- Politically exposed persons and their related parties
- Customers residing in or having transactions to/from countries considered by the EU to be high-risk third countries
- Correspondent banks and similar business connections
- Persons suspected of having committed financial crimes, money laundering, terrorist acts or appearing on an official sanctions list
- Customers considered specifically to be associated with a high risk for the Bank – either with respect to money laundering, terrorist financing or financial crime.

Sydbank must have efficient systems for screening the customer database at regular intervals against applicable sanctions lists so as to ensure the freezing of a customer's funds if the screening shows an identity match.

4.2 Products

To the extent possible the Bank's products must be developed so that they cannot be used for money laundering and terrorist financing. Furthermore they must be offered in such a manner so that transactions via the Bank cannot be carried out anonymously.

Selected products are offered exclusively to persons and businesses that establish a customer relationship with the Bank or that are already customers:

- Safe-deposit boxes
- Currency conversion and currency disbursements.

4.3 Transactions

Sydbank does not carry out transactions for persons and businesses that do not have a customer relationship with the Bank.

Transactions are generally not carried out to North Korea, Iran, Syria and the Crimea.

4.4 Transaction monitoring

Sydbank must have efficient systems and procedures for screening transactions against applicable sanctions lists so that payments can be withheld and frozen if a screening shows an identity match. Transaction Monitoring – AML is responsible for screening transactions.

Furthermore Sydbank must strive at all times to 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, the expected scope and that the customer's transactions do not differ from those of similar customers in other respects. 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 an investigation of a customer relationship has been made and in the event that a report has been filed in accordance with the Danish Money Laundering Act.

4.5 Supply channels

The establishment of customer relationships and the supply of products to the Bank's customers must take place wherever possible in such a manner to make it impossible for the Bank to be used for money laundering and terrorist financing. In addition the supply channel must to the extent possible be established so that the Bank has knowledge of by whom the channel is used.

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. Quality Assurance – AML & GDPR makes sure that the internal guidelines are accessible, understandable, updated and approved by AML Risk Management.

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.

All employees at the Bank are under an obligation to report any suspicion that the Bank is being used for money laundering or terrorist financing:

- Any suspicion with regard to specific customers is reported to Transaction Monitoring – AML.
- Any flaw in the measures to prevent the Bank from being used for money laundering and terrorist financing is reported to AML Risk Management.
- The Group Executive Management and key employees are obliged to report to the Board of Directors and the Group Executive Management respectively if they receive warnings from authorities and similar that the Bank is being used for money laundering or terrorist financing.

6. Collection, storage and sharing of information

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 is shared internally in the Bank only 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 that must be investigated further and that may result in the Bank notifying the authorities in Denmark as well as Germany. Furthermore information is shared when controls are implemented in connection with the Bank's risk management.

Collected information, documents and registrations are passed on to the Danish Money Laundering Secretariat (the State Prosecutor for Serious Economic and International Crime) as stipulated in the Danish Money Laundering Act or related legislation.

Finally necessary information is passed to the Danish FSA where it carries out inspections and investigations at the Bank. Sydbank is always accommodating

and cooperative when contacted by the Danish FSA so that the Bank does not hinder supervisory activities conducted by the Danish FSA.

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

7. Approval and update of the Policy

AML Risk Management is responsible for ensuring on an ongoing basis necessary updates of this Policy and that it is submitted 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 as well as the appendix "Risikotolerance – Hvidvaskloven og sanktionsregler" ("Risk tolerance – Money Laundering Act and sanctions rules"). Following approval the Policy will be made available on the Bank's website in Danish, German and English and on the Bank's intranet. The guidelines of the appendix are incorporated into the relevant business procedures and are only available on the Bank's intranet.