Danske Bank

AML, CTF and Sanctions Policy

SEPTEMBER 2018

1. Purpose and Objective

The purpose of this policy is to set the high-level principles and standards of management of financial crime risks, including money laundering, terrorist financing and sanctions breaches, for Danske Bank Group (the Group) and constitutes a part of the Board of Directors' Instructions to the Executive Board.

The objective of this policy is to ensure regulatory compliance and to establish an internal framework that minimizes the risk of sanctions breaches and abuse of the Group's products and services for money laundering and terrorist financing purposes. This is in alignment with the Group strategy and The Essence of Danske Bank, which sets the Group's vision to be recognized as the most trusted financial partner.

2. Scope and application

The Policy applies to all employees and persons in a comparable position, all functions, all units in Danske Bank A/S, and all regulated subsidiaries, once adopted by their Senior Management

In case a Group olicy conflicts with local requirements, Senior Management of the subsidiary can approve a Group policy with deviations. Any material deviations from the Group policy must be reported to the Board of Directors of Danske Bank A/S as well as the administrator of the Information Management Policy.

The aim of the Group is not only to comply with relevant legal requirements, but also to mitigate and reduce the potential risk to the Group of our customers using our products, services and delivery channels to launder the proceeds of illegal activity, fund terrorist activity or perform transactions in breach of financial sanctions.

3. Target group

This Policy is relevant to all employees and persons in a comparable position in the Group.

4. Requirements

The Group must comply with the relevant laws and regulations in the Market Areas in which it operates and may, based on its risk tolerance, adopt more exacting standards. The Group must comply with the requirements set out in the:

- National provisions transposing Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing
- Applicable sanctions regimes
- Any other law or regulation applicable to the Group's operations.

5. Definitions

Money laundering and terrorist financing

For the purpose of this Policy, the act of Money Laundering shall have the same meaning as provided in Article 1(3) of the EU AMLD IV, which provides that it, when committed intentionally, encompasses;

- (a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
- (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
- (c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
- (d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country."

For the purpose of this Policy, the act of Terrorist Financing shall have the same meaning as provided in Article 1(5) of the EU AMLD IV, which provides that it encompasses; "the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA".

For the purpose of this Policy *the act of Terrorist financing* refers to the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out an act of terror, or that the funds will be used to support any terrorist group, persons or association.

Financial sanctions

Financial sanctions are measures imposed by national governments and multinational bodies which seek to alter the behaviour and decisions of other national governments or non-state actors that may (i) threaten the security of the global community, or (ii) violate international norms of behaviour (e.g. human rights violations).

The Group must comply with the following sanctions measures:

1. The United Nations (UN) Security Council consolidated sanctions list;
2. The EU's consolidated list of persons, groups and entities;
3. The US Department of the Treasury, Office of Foreign Assets Control (OFAC) sanctions lists:

4. The US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) list;
5. The UK HM Treasury (HMT), Office of Financial Sanctions Implementation, "consolidated list of targets"

Financial Crime

For the purpose of this policy, *Financial Crime* is used as the collective term for Money Laundering, Terrorist Financing and Violations of Financial Sanctions.

Risk Based Approach

The Group shall apply a Risk Based Approach (RBA) to AML/CTF. The RBA encompasses identifying, assessing and understanding the ML/TF risks to which the Group is exposed and to take measures proportionate to those risks for the purpose of mitigating them effectively. This means that the range, degree, frequency or intensity of controls will be more comprehensive in situations assessed as posing a higher ML/TF risk while these measures will be reduced in situations assessed as posing a lower ML/TF risk. Applying a RBA, thereby, allows the Group to target its resources in the most efficient manner. Situations assessed as posing a lower risk must never imply that control measures are not applied.

6. Group measures towards money laundering/terrorist financing and financial sanctions

The Group is undertaking a number of initiatives to strengthen its ability to ensure its compliance with the requirements outlined in this Policy. The Group will, therefore, continually assess its existing policies, procedures, controls and IT system and make necessary changes so as to be most effective in accordance with the risk based approach.

Governance

Through this Policy, the Board of Directors have instructed the Executive Board to ensure that there is a robust approach within the Group to prevent money laundering, terrorist financing and breaches of financial sanctions. It is the responsibility of the Executive Board to ensure that the Group complies with the measures set forth in this Policy. The Executive Board is, furthermore, responsible for implementing this Policy and may delegate its responsibilities. The Executive Board shall appoint an "anti-money laundering responsible person" at management level with the responsibility to ensure that the Group complies with the legal requirements.

The Business Units, *as the first line of defence*, are accountable for the risks related to financial crime. Business Units as well as Senior Management can delegate tasks related to the mitigation of financial crime risks to Group Operations or other first line departments. However, delegating will not change the risk ownership and accountability for Business Units but will merely imply a new responsible unit for conducting the delegated process.

Group compliance, *as the second line of defense*, is responsible for the monitoring, assessment, guidance and reporting of money laundering, terrorist financing and financial sanctions risks.

Internal Audit – *as the third line of defence* – is responsible for carrying out independent testing of the Group's policies, procedures and controls.

Outsourcing to external suppliers may only be executed after close consultation with Group Compliance and in accordance with the Outsourcing Policy.

Risk tolerance

The Group does not tolerate any breach of the requirements set forth in this Policy that could jeopardise the soundness and integrity of the Group or damage the public trust and confidence in the financial system as a whole.

Any material or systemic breaches must be reported to the Audit Committee.

The Group does not accept any business relationship with a designated person, group and entity subject to financial sanctions set out in 3.3.

In order to comply with financial sanctions regulations, the Group must be able to verify the identity of its customers. Therefore the Group requires a robust control environment with low error rates for due diligence after applying internal controls.

The Group will examine all legal possibilities to satisfy the requirements set forth in this Policy and, at the same time, comply with the requirements of other internal policies and legal requirements. Should a conflict arise between the requirements within this Policy and any other Policy or legal requiremnt, Group Compliance shall be consulted.

The Group will take all relevant steps to reduce the provision of products and services to natural persons and/or legal entities where the Group has a reason to suspect that the natural person and/or the legal entity is or will use the Group's products and/or services for financial crime.

Group wide risk assessment on financial crime

The Group operates in several Market Areas with a full range of banking products being offered to multiple customer segments. Accordingly, the Executive Board must establish an overall group wide risk assessment on financial crime describing the inherent financial crime risks of the Group, the control environment to mitigate such risks, and the residual financial crime risk.

The group wide risk assessment on financial crime represents a cornerstone for the Group in meeting the requirements of the risk-based approach.

Customer due diligence

The Group's goal of developing its knowledge of its customers so as to improve the value of advice it can offer is closely related to the due diligence obligations of the Group. In parallel to the verification of a customer's identity, the Group applies a risk based approach towards the collection, registration, and monitoring of information in relation to the nature and intent of the customer relationship.

The data gathering, which is conducted to meet the abovementioned requirements, forms the baseline for transaction monitoring and constitutes a foundation in the Group's IT-driven AML, CTF and financial sanctions risk scoring model ("Risk Scoring").

The Group shall apply a risk based approach towards due diligence through the Risk Scoring with reference to a customer's geographic ties, chosen products and / or services, delivery channels and customer specific factors.

The Group will decide upon appropriate customer acceptance instructions in order to set clear guidance as to which natural persons and legal entities the Group will see as the strategic customer base with references to AML, CTF and financial sanctions risk. These instructions should also give guidance as to the procedure for terminating a customer relationship due to financial crime concerns.

Given the volume of customers in many Market Areas, the Group requires a robust and effective IT solution to cater for an effective initial registration and ongoing monitoring of the customer base. It is essential that all natural persons and legal entities are registered on the Group's IT systems. Having sufficient identification information, the Group will - within the purpose of the requirements - aggregate all relevant products and services on each customer number.

The Group undertakes significant effort to determine the ownership and control structure of legal entities. Therefore, the Group must identify and verify the identity of any natural persons who ultimately owns or controls the customer.

Screening of politically exposed persons
In order to ensure that all natural persons defined as politically exposed persons ("PEPs") are identified and registered in the Group's system as such, a PEP screening process is conducted when natural persons are on-boarded. Furthermore, the customer database is screened for PEPs on an ongoing basis.

Enhanced Due Diligence and Ongoing Due Diligence
The Group performs enhanced due diligence and on-going due diligence measures proportionate with the Risk Scoring of the customer. High risk customers will therefore be subject to enhanced due diligence and annual on-going due diligence. Ongoing due diligence processes will be applied to all existing customers within a specific period that will determine by whether they are scored as *medium* or *low*.

Design
The Group IT solution must be designed to ensure that robust internal controls of customer due diligence are maintained.

This requires strong data quality and, where possible, automatic ongoing due diligence between public registries and the Group's IT systems in relation to customer data. Data quality shall be measured and reported as a key performance indicator.

Transaction monitoring

The Group applies a risk based approach to transaction monitoring which includes automated as well as manual processes. Transaction monitoring is conducted in order to evaluate whether the activities of the customer (the use of their products and/or services and/or their general behaviour) is consistent with the obtained information on the purpose and intended nature of the business relationship.. As part of its transaction monitoring, the Group further investigates activities that are deemed to be "unusual" with regard to the stated position of the customer.

The automated transaction monitoring shall, based on a risk based approach, cover all Business Units, all customers, all market areas and all products with appropriate scenarios. The manual transaction monitoring – investigating and reporting of the unusual activity to the Money Laundering Reporting Officers - is achieved through training and awareness campaigns.

Design

The Group performs automated transaction monitoring. Likewise a process has been established where Business Unit employees can file "unusual activity reports" with the Money Laundering Reporting Officers based on information gained from automated and manual transaction monitoring. The Money Laundering Reporting Officers are responsible for assessing whether the described activities in the "unusual activity report" are genuinely suspicious and warrant the filing of a "suspicious activity report" to the local Financial Intelligence Unit.

Sanctions

In order to comply with sanctions imposed by the UN, EU, US, and any local authorities, relevant control procedures must be in place. Most Market Areas within the Group are EU Member States and, as such, are obligated to follow EU regulation and, therefore, comply with EU sanctions.

US sanctions regulations have a major impact on the Group due to the USD transactions that the Group undertakes. The Group has therefore chosen to be compliant with the requirements of the Office of Foreign Asset Control ("OFAC"), regardless of currency.

The Group has a screening solution, which is integrated in the Group's IT systems to ensure that the Group is compliant with AML, CTF and financial sanctions regulations.

The Group establishes a Sanction Board where principal decisions are to be taken regarding Sanctions. The mandate includes decisions on deviations from requirements of the Policy extending the regulatory requirements. If Group Compliance disagrees to the decision of the Sanction Board the decision has to be escalated to the head of the Business Unit.

Transaction screening

The Group conducts real-time transaction screening on all transactions in relation to relevant lists of designated persons, groups and entities subject to financial sanctions..

Customer screening

The customer screening solution ensures that all customer registered in the Group's IT systems, including natural persons, legal entities and their beneficial owners, are screened against the relevant sanctions lists of designated persons, groups and entities.

Persons, groups and/or entities designated by the UN and EU shall be highlighted and may be subject to asset freezing with subsequent reporting to appropriate authorities. The Group will, terminate or limit the services offered to natural persons and legal entities designated by OFAC as Specially Designated Nationals.

Management information

The ExBo must determine key performance indicators ("KPIs") and develop management information requirements and processes to gain insight into, and satisfaction with, the effectiveness of the AML, CTF and sanctions compliance framework.

Retention and record keeping

For the purpose of preventing, detecting and investigating unusual and suspicious transactions, the Group must keep electronic records of all transactions and due diligence measures carried out in accordance with this Policy.

Records must be kept in a manner making information and documents available to all employees having appropriate access to the customer in question (within the Group's existing IT solution).

Documentation must be kept during the lifetime of the customer's relationship with the Group and at least *five* years after termination of the customer relationship or after the date of an occasional transaction.

Training and awareness

The Group requires that all employees possess an adequate awareness level of the risks of financial crime. The Group must ensure that all employees have a suitable degree of awareness, i.e. when staff encounter something unusual relating to a customer's behaviour in their daily work, they must consider whether the unusual behaviour may be related to ML, TF and/or sanction evasion.

In relation to the training of employees, the Group applies a RBA so that the broad range of employees can have their training through yearly e-learning courses targeted towards the job position of the employee. By acknowledging the complexity of this area, the Group supports external certification and face-to-face training for employees working in key positions in this area of the Group.

7. Escalation

The Group has an Escalation Policy stating the requirements for appropriate and timely internal reporting of potentially problematic cases across Danske Bank Group. The requirements in the Escalation Policy must always be considered in relation to violation of the Group's obligation to prevent and mitigate financial crime with adherence to other related policies and governing documents.

8. Reporting

The Executive Board must determine key performance indicators and develop management information requirements and processes to gain insight into, and satisfaction with, the effectiveness of the AML, CTF and sanctions compliance framework.

9. Review

This Policy must be reviewed by Group Compliance at least annually. Any changes to the Policy must be endorsed by the Executive Board, the Audit Committee and approved by the Board of Directors.

The key stakeholders and subject matter experts who have provided input for and endorsed Policy: Financial Crime Compliance