Danske Bank

Group Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Policy

29 April 2020

1. Objective

The objective of the Group Anti-Money Laundering ("AML"), Counter-Terrorist Financing ("CTF") and Sanctions Policy ("the Policy") is to set out the principles for the management of risk and compliance associated with money laundering ("ML"), terrorist financing ("TF") and sanctions in Danske Bank A/S ("the Group").

The Policy is designed to ensure that the Group adheres to:

- All applicable laws and regulations in relation to AML and CTF for the jurisdictions in which it operates; and
- All relevant sanctions regimes in all jurisdictions in which it operates. These include EU, UN and any other applicable sanctions as appropriate, as well as US sanctions to the extent they have extraterritorial application or risk implications for the Group's business activities.

This Policy must be reviewed annually, or more frequently if required.

2. Definitions

The following definitions apply to the terms used throughout the Policy:

Term	Definition
Money laundering	Money laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source.
Terrorist financing	Terrorist Financing is the provision or collection of funds with the intention that they can be used to carry out an act of terror, or that the funds will be used to support any terrorist group, persons or associations in any ways.
Sanctions	Sanctions are restrictions or prohibitions imposed by laws and regulations which can target economic, diplomatic, financial and trade activities with specific countries, governments, entities, organisations and/or individuals. Governments and supranational organisations implement sanctions to achieve various foreign policy objectives, such as to promote and maintain international peace and stability, democracy and human rights, to prevent terrorism, proliferation of arms and weapons of mass-destruction.
Senior Management of the Group	Senior Management constitute the members of the Board of Directors and the Executive Leadership Team.

Politically-Exposed-Persons (PEPs)	PEPs are natural persons (and their close associates and family members) who have, or have previously held, a high political profile, or a prominent public function. A more detailed definition can be found in the AML and KYC Instruction.
EU High Risk Third Country List	The EU High Risk Third Country List is published by the EU and includes those countries with strategic deficiencies in their national AML and CTF that pose substantial threats to the EU and its financial system.

3. Scope

The principles of this Policy set the Group's approach for compliance with AML, CTF and Sanctions related laws, regulations and other requirements that are applicable to the Group and its operations.

3.1. Target Group

This Policy applies to all employees (including temporary employees) in all functions, all units in the Group and all subsidiaries as well as all third parties acting on behalf of the Group.

Subsidiaries and branches may deviate from this Policy if it conflicts with local regulatory requirements. The Policy administrator in the subsidiary or relevant representative from a branch should justify the rationale behind the deviation and ensure that the administrator of this Policy is consulted and endorses any deviation. If any subsidiaries or branches deem the Policy not relevant, it must be agreed with and endorsed by the administrator of this Policy.

The administrator of this Policy must document and report any deviations from the Policy to the Executive Leadership Team of Danske Bank A/S via the administrator of the Steering Policy. The Executive Leadership Team should report all deviations from Group Policies to the Board of Directors of Danske Bank A/S.

3.2. Breaches

Lack of adherence to this Policy may have severe consequences to the Group and its employees including:

- Violating AML, CTF and Sanctions laws and regulations;
- Receiving monetary fines, criminal penalties, and/or regulatory enforcement orders; and
- Exposing the Group to reputational risk.

A breach is defined as non-compliance with any requirement in this Policy which has not been approved. All breaches must be reported to Group Compliance within five days of discovery.

Lack of adherence to this Policy may also lead to disciplinary action up to and including potential dismissal.

4. Policy Content

Principle 1: The Group must maintain a governance framework that clearly defines roles, accountabilities and responsibilities for AML, CTF and sanctions compliance

The Group must develop a governance framework that is promoted and maintained across all areas of the Group that includes:

- Clearly allocated accountabilities and responsibilities to manage ML, TF and sanctions risk;
- An appointed AML responsible member from the Executive Leadership Team, an AML Responsible Compliance Officer and an AML responsible person in the First Line of Defence;
- A strategy from Senior Management that actively promotes a strong AML, CTF and sanctions compliance culture;
- Governance that sets out appropriate mandates, authorities and oversight capabilities; and
- Adequate resources in respect of personnel, competency and technology.

The Group must set out the responsibilities that all employees have in the management of ML, TF and sanctions risk. The governance framework must also include the specific accountabilities held by the relevant bodies and functions within the governance structure, including the Senior Management, Group Compliance and the Business Units.

Principle 2: The Group must apply the Three Lines of Defence Model to ensure effective governance and oversight of ML, TF and sanctions risk

The Group applies the Three Lines of Defence Model in accordance with the Group's Enterprise Risk Management approach. The Three Lines of Defence Model is a key element in ensuring effective governance and oversight of ML, TF and sanctions risk, including having clearly defined roles and responsibilities in place.

The Group's frontline units and their direct support functions within the Business Units constitute the First Line of Defence and are accountable for identifying, mitigating and managing ML, TF and sanctions risk associated with customers, products and services. This includes designing, implementing and executing controls and processes to identify and manage ML, TF and sanctions risks within their business and operations and performing ongoing oversight on the effectiveness of these controls and processes.

Group Compliance constitutes part of the Second Line of Defence. Group Compliance is responsible for ensuring the Group has adequate and robust policies and instructions addressing AML, CTF and sanctions compliance, while also monitoring, supporting, advising and challenging First Line of Defence compliance and risk management practices.

Group Internal Audit constitutes the Third Line of Defence. The scope of Internal Audit's mandate is unrestricted and includes oversight of the activities conducted by both the First and Second Lines of Defence.

Principle 3: The Group must have sufficient management information and reporting to monitor and oversee the management of risks associated with ML, TF and sanctions

The Group must produce key performance/risk indicators and develop management information ("MI") requirements and processes to maintain effective and meaningful oversight of the Group's management of the risks associated with ML, TF and sanctions.

Principle 4: The Group must apply a risk-based approach to ensure that risk mitigation measures are proportionate to the level of associated ML, TF and sanctions risk

The Group must apply a holistic, risk-based approach to ensure that effective controls are in place that are proportionate to the identified ML, TF and sanctions risk. The Group must identify and assess its ML, TF and sanctions risk to enable the effective design and implementation of controls to manage and mitigate these risks in line with the Group's ML, TF and sanctions risk appetites.

Principle 5: The Group must conduct a risk assessment to identify and measure the inherent risk of ML, TF and sanctions and evaluate the design and effectiveness of controls to determine the Group's residual risk

The Group must complete a risk assessment, at least annually, to identify and measure the inherent risk of ML, TF and sanctions and evaluate the design and effectiveness of controls to determine the Group's residual risk.

The risk assessment must adequately account for the potential ML, TF and sanctions risk arising from all relevant factors, including the Group's customers, products, services, delivery channels, supply chain, intermediaries, counterparties, transactions and geographic locations. The risk assessment must also be proportionate to the size and complexity of the Group and its operations.

The risk assessment results inform the design, development, maintenance and implementation of its AML, CTF and sanctions policies and procedures and other mitigation activities.

Principle 6: The Group must maintain a control framework that enables effective and efficient mitigation of ML, TF and sanctions risk

The Group's internal control framework must identify, manage and mitigate ML, TF and sanctions risk. The framework must set clear expectations that include:

- Monitoring, identifying and managing ML, TF and sanctions risk;
- Investigating and reporting potential ML, TF or violations of sanctions;
- Defining and documenting risk-based control procedures and processes pertaining to AML, CTF and sanctions; and
- Regularly testing the controls to ensure effective operation as well as being appropriate and proportionate to the associated ML, TF and sanctions risk.

The framework includes screening, monitoring and due diligence controls that take into account relevant risk factors associated with customers, industries, geographies, typologies, products and service channels and most typically a combination of these.

Principle 7: The Group must perform due diligence measures when establishing and maintaining relationships with customers

The Group's customer due diligence framework must ensure that all customers are subject to due diligence measures prior to establishing a relationship and throughout the customer relationship. The due diligence measures must be completed prior to carrying out any transactions on behalf of the customer. Further, each customer must be owned by a specific Business Unit which remains accountable for the ongoing oversight of that customer.

The Group must ensure that all customers are subject to an appropriate level of due diligence at the time of on-boarding and during the duration of the customer relationship, in accordance with their risk-rating and the Group's other policies, instructions and procedures.

Subprinciple 7.1: The Group must not establish or maintain relationships where it cannot obtain sufficient information, or mitigate the risks associated with the customer or other parties

The Group must not establish a relationship with customers or other parties where it has not obtained all relevant information as required by the due diligence requirements or where it has been unable to complete the due diligence processes.

Further, the Group must not maintain relationships with prohibited customers such as shell banks.

Subprinciple 7.2: The Group must perform enhanced due diligence measures where the business relationship with the customer is assessed to pose an increased ML, TF and sanctions risk

The Group must apply enhanced due diligence measures on customer relationships that expose the Group to a higher ML, TF and sanctions risk. This requires Business Units to collect and assess additional information/documentation in relation to the customer to ensure the application of appropriate controls and that the relationship is within the Group's ML, TF and sanctions risk appetites.

Subprinciple 7.3: The Group must develop procedures to manage relationships with other areas of the Group or third parties that carry out aspects of the AML, CTF and sanctions framework on its behalf

The Group must develop and implement appropriate standards when relying on, or outsourcing ML, TF and sanctions risk management activities to other parties, both internally and externally. Further, whilst AML, CTF and sanctions responsibilities can be performed by third parties, the Group remains ultimately accountable for their activities.

Subprinciple 7.4: The Group must identify and manage risks associated with customers and relevant parties that are considered PEPs

The Group must develop, implement and maintain effective measures and processes to identify and mitigate the risks associated with PEPs.

Further, the Group must maintain an appropriate definition of a PEP that meets regulatory standards, as well as establish PEP specific due diligence measures and controls.

Subprinciple 7.5: The Group must have controls to manage ML, TF and sanctions risks associated with correspondent relationships

The Group must develop and maintain specific enhanced due diligence measures and controls relating to correspondent relationships, enabling an effective and consistent risk-based approach across the Group.

Subprinciple 7.6: The Group must have controls to manage ML, TF and sanctions risks associated with countries on the EU High Risk Third Countries List

The Group must conduct enhanced due diligence on customers carrying out transactions with, or maintaining a registered office address in/residing in, countries on the EU High Risk Third Countries List.

Subprinciple 7.7: The Group must perform ongoing due diligence on all customers to ensure that customer information is accurate and up-to-date

The Group must perform ongoing due diligence ("ODD") on all customers consisting of periodic reviews and ongoing monitoring of their activity. This enables the Group to assess whether the customers'

activities correlate with the information provided by the customer at on-boarding or when ODD was last performed, and to detect any suspicious customer activity. Performing ODD also enables the Group to ensure that the controls and due diligence measures applied on the relationship continue to be adequate.

Minimum frequency for ODD is determined by the risk-rating associated with the customer or where circumstances or events associated with the customer trigger an event driven ODD review.

Principle 8: The Group must conduct monitoring and screening to identify ML, TF and sanctions risk

The Group must develop and implement transaction monitoring and screening controls to identify its sanctions exposure, potential suspicious activity, PEP relationships and potential adverse media.

Subprinciple 8.1: The Group must conduct risk-based transaction monitoring to identify ML and TF

The Group must monitor all customer relationships on an ongoing basis and review customer transactions to identify activity that is inconsistent with their profile and/or nature of business. Due to the significant volume of transactions processed, the Group must develop risk-based scenarios, typologies, rules and thresholds to identify such activity.

Subprinciple 8.2: The Group must apply risk-based sanctions screening against relevant sanctions lists

The Group must screen all relevant information related to customers, potential customers, associated parties, transactions and business activities against relevant sanctions lists to ensure compliance with sanctions.

The Group must ensure that the screening controls are applied prospectively prior to engaging in a relationship or a transaction and that any potential sanctions-related alerts and concerns identified through application of those controls are resolved prior to completing the engagement or transaction.

Subprinciple 8.3: The Group must conduct screening to identify which customers should be classified as PEPs

The Group must ensure that all customers are screened against PEPs lists to determine whether there are any PEPs or close associates of PEPs within the Group. If hits are identified, these should be investigated to determine whether they are genuine and if so, appropriate due diligence should be applied.

Subprinciple 8.4: The Group must conduct risk-based searches to help identify potential adverse media relating to its customer relationships

The Group must apply risk-based media searches to help identify whether any customers, potential customers or relevant associated parties are the subject of financial crime related adverse media. Relevant hits should be investigated to determine whether they are true and if so, their materiality in respect of the relationship with the Group.

Subprinciple 8.5: The Group must maintain a list management framework to ensure up-to-date and accurate screening for sanctions and PEPs

The Group must establish a list management framework and governance that defines the relevant internal and/or external sanctions and PEP lists to be applied in screening. This includes the development of appropriate list management processes to ensure that all lists used for screening are accurate and up-to-date.

Principle 9: The Group must ensure that suspicious activity or potential sanctions violations are investigated and reported to the relevant authorities

The Group must ensure that it implements and maintains effective controls and processes to ensure that suspicious activity or potential sanctions violations are reported to the appropriate authorities in a timely manner.

Subprinciple 9.1: The Group must investigate and report knowledge or information of transactions, assets or activities that are suspected to be or have been connected to ML or TF

The Group must ensure that if there is any concern relating to transactions, assets or activity that may be connected to money laundering or terrorist financing, this must be investigated and reported to the Suspicious Activity Reporting Office ("SARO") as an Unusual Activity Report ("UAR"). The investigation process should include controls to prevent the customer being tipped off.

Where the unusual activity is determined to be suspicious, the relevant SARO or Money Laundering Reporting Officer must report the activity to the relevant local Financial Intelligence Unit ("FIU") or authority.

Subprinciple 9.2: The Group must investigate potential sanctions violations to determine appropriate action, and when necessary, report those to the relevant authorities

The Group must ensure that potential sanctions violations or material sanctions concerns are reviewed by Group Compliance to determine whether it requires further action. Any action taken will depend on the applicable sanctions implicated by the concerns. These may include, among others, freezing of funds, rejecting a transaction or declining a relationship and reporting to authorities.

Where a transaction, relationship or other activity is determined to be subject to applicable sanctions Group Compliance must report it to the relevant authority.

Principle 10: The Group must ensure that its employees have adequate competence and awareness about AML, CTF and sanctions requirements and controls by providing regular training and communication

The Group must provide employees, including Senior Management, with training on ML, TF and sanctions risk. This includes specific, tailored training for employees that fulfil roles with higher ML, TF and sanctions risk exposure.

Training is an integral part of the Group's ML, TF and sanctions risk management. Completion of training must be monitored through appropriate MI metrics, and non-completion of training must be taken seriously through appropriate consequence management.

Principle 11: The Group must ensure that records relevant for AML, CTF and sanctions are retained to ensure auditability and investigation

The Group must retain electronic records concerning customer information, transactions, reviewing and investigation of alerts and other relevant information, including material decisions, approvals and documentation related to the management of ML, TF and sanctions risk.

All records must comply with relevant data retention, data privacy and data protection laws and regulations. At minimum, all records should be kept for a period of five years from the date the customer relationship ended or a one-off transaction was processed.

Principle 12: The Group must assess and monitor the effectiveness of its AML, CTF and sanctions framework through regular assurance testing including audits

The Group must regularly conduct risk-based assurance testing of its AML, CTF and sanctions framework. The methodologies and frequency of testing should be appropriate to the level and sophistication of the risks.

The Group must ensure that the functions performing assurance activities have sufficient skills, expertise, resources and authority within the organisation to effectively identify weaknesses and deficiencies, inform enhancement opportunities as well as inform the ML, TF and sanctions risk profile for the purposes of management reporting.

Principle 13: The Group must ensure that all AML, CTF and sanctions processes and technologies are managed through relevant business continuity plans and processes

AML, CTF and sanctions controls and processes are interlinked with the ability to process transactions, deliver products and services, and on-board and maintain customers and other relationships. Any disruption in controls and processes may have a significant impact on the Group's compliance with its AML, CTF and sanctions obligations, but may also result in significant business and market disruptions.

As it is critical to ensure compliance while also ensuring that the Group continues to provide and deliver services, the Group must ensure that all critical AML, CTF and sanctions related controls and processes have appropriate business continuity plans and protocols implemented to ensure compliance and avoid business disruptions.

Principle 14: The Group must engage, cooperate and communicate with supervisors, competent authorities and law enforcement agencies

Group Compliance must be immediately informed of any ML, TF and sanctions related request received from a supervisory body, regulatory authority or law enforcement agency. Group Compliance must ensure that all information requests are promptly responded to and managed in accordance with relevant data protection and bank secrecy requirements, as necessary.

5. Escalation

The Group's Escalation Policy sets the requirements for internal reporting of potentially problematic cases across the Group. The requirements in the Escalation Policy must always be considered in relation to violation of the Group's obligation to prevent and mitigate ML, TF and violation of sanctions, with adherence to other related policies and governing documents.

Please refer to the Group's Escalation Policy and Common Escalation Matrix for Potentially Problematic Cases Directive.