Policy on Anti-Money Laundering and Combating Financing of Terrorism for the SEB Group

derived from the Rules of Procedure of the Board of Directors

adopted by the Board of Directors of
Skandinaviska Enskilda Banken AB (publ)
on 26 January 2022

Group Compliance

1. Introduction

Money Laundering (ML) and Terrorist Financing (TF) are international problems that constitute a serious threat against the financial system and by extension also against the real economy and public security. Combating ML/TF is a priority for Skandinaviska Enskilda Banken AB (publ) (SEB) and its branches and subsidiaries (hereinafter jointly referred to as 'SEB Group') in order to prevent the SEB Group from being used to facilitate the movement of criminal proceeds or transfer of funds destined to finance terrorism. SEB Group has a responsibility to protect its customers and shareholders, but also the integrity and the stability of the international financial system.

Compliance with the Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) regulation is a key part of the SEB Group's customer risk tolerance framework in order to achieve consistent and robust AML/CFT compliance globally in all jurisdictions where the SEB Group operates.

Where ML/TF risks are referred to in this Policy, risks in relation to other types of financial crime may also be relevant. Such risks include, but are not limited to, Financial Sanctions (FS), and Bribery and Corruption (BC). Where relevant, the requirements of this Policy may contribute to the mitigation and management of these risks. As the areas of ML/TF and FS risks are closely related, this Policy should be read in conjunction with the SEB Group's Policy on Financial Sanctions.

2. Purpose and scope

Through this Policy, SEB's objective is to ensure compliance with the SEB Group's regulatory obligations and mitigate and manage ML/TF risks by defining clear principles and requirements based on SEB's risk tolerance. Therefore, this Policy provides a consistent set of risk management principles and minimum mandatory requirements which shall be established, maintained and implemented across the SEB Group in order to prevent, detect and take proper action against ML/TF. Furthermore, the risk management principles and minimum requirements shall protect the SEB Group from violating AML/CFT laws and regulations which could lead to reputational damage, regulatory remarks, fines or other enforcement actions.

The SEB Group shall comply with all requirements in this Policy. SEB, branches and subsidiaries shall take necessary steps to implement this Policy, taking local or sector specific rules into account where relevant.

3. AML/CFT policy statement

The SEB Group shall, as part of its normal business conduct, combat ML and TF. This is of utmost importance in order to meet regulatory obligations, to maintain the SEB Group's good reputation, and to contribute to the stability of the financial system. The SEB Group shall also apply high ethical standards and assume social and environmental responsibility.

SEB is committed to complying with all applicable AML/CFT laws and regulations in the jurisdictions in which it operates. SEB shall have processes and procedures in place to identify and manage the ML/TF risks that it is exposed to and take proportionate and adequate measures to manage these.

The amount and type of ML/TF risk that the SEB Group is willing to tolerate, and the types of activities and relationships that are acceptable, shall be defined in the customer risk tolerance framework and approved by the Group Risk Committee. The SEB Group will not establish or maintain relationships with customers or other parties, nor offer products or services which are defined as prohibited or otherwise fall outside of the SEB Group's ML/TF risk tolerance or are prohibited by applicable AML/CFT laws and regulations.

4. The SEB Group's AML/CFT Risk Management Governance Model

The SEB Group's AML/CFT Risk Management Governance Model shall be based on a three lines of defence approach. Effective AML/CFT risk management requires proper governance and the establishment of clearly defined roles and responsibilities across SEB's three lines of defence and SEB's senior management. SEB will ensure that roles and responsibilities for AML/CFT risk management are clearly defined, documented and implemented accordingly and as set out in the Operational Model in the *Instruction for Internal Governance* for the SEB Group.

The SEB Group's AML/CFT risk management governance model shall include governing and decision-making roles, functions, committees and working groups to address AML/CFT risk management matters on a group-level in order to achieve necessary and consistent oversight and decision-making capabilities across divisions, legal entities and jurisdictions. Such roles, functions, committees and working groups will have documented mandates and include senior level representation from the first and second lines of defence, where appropriate. The responsibilities and given mandates to the different roles, functions, committees and working groups shall be defined and documented in appropriate AML/CFT instructions and AML/CFT governance model.

As the areas of ML/TF risks and FS risks are closely related, the roles, functions, committees and working groups mandated within AML/CFT risk management may also be governed by the *Financial Sanctions Policy for the SEB Group, Instruction for procedures to handle Financial Sanctions for the SEB Group* and the *First Line FS Governance Model*, and such should be read in conjunction with the documented mandates given within sanctions risk management.

4.1 *The Board of Directors*

The Board has the overall responsibility for the management of the affairs and the organisation of the SEB Group. In respect of the area of AML/CFT this includes ensuring that adequate and effective internal controls for the management of ML/TF risks have been set and implemented and that there are sufficient resources to effectively manage ML/TF risks.

4.2 *The President and Chief Executive Officer*

The President and Chief Executive Officer (the "President") is responsible for the implementation of effective ML/TF risk management practices and controls in both first and second line of defence, and to ensure that these are implemented consistently throughout the SEB Group. This is to enable the SEB Group to effectively assess, manage, control and oversee ML/TF risks and to meet the requirements of this Policy.

In order to effectively control the ML/TF risks to which the SEB Group is exposed, and support the consistent implementation of this Policy throughout the SEB Group, the President holds the responsibility for ensuring that a necessary accompanying global group-wide AML/CFT instruction with minimum requirements for ML/TF risk management activities within the SEB Group (the *Instruction for procedures against Money Laundering and Terrorist Financing for the SEB Group*) is defined, documented and adopted.

4.3 *Group FCP Senior Manager*

The President shall appoint a Group FCP Senior Manager who shall have the overall responsibility for the implementation of Financial Crime Prevention (FCP) requirements in the SEB Group, The responsibilities of the FCP Senior Manager in relation to AML/CFT are further detailed in the *Instruction for procedures against Money Laundering and Terrorist Financing for the SEB Group*, .

4.4 *Group FCP Committee*

The SEB Group shall have a Group FCP Committee, chaired by the Group FCP Senior Manager. The Group FCP Committee shall make decisions on the SEB Group's activities within the FCP area within the given mandates. The responsibilities of the Group FCP Committee in relation to AML/CFT are further detailed in the *Instruction for procedures against Money Laundering and Terrorist Financing for the SEB Group*

4.5 *Group Compliance*

Group Compliance is a SEB Group-wide function that is independent from the business activities and forms part of the second line of defense. The Group Compliance function shall ensure the quality of compliance in the AML/CFT area through information, advice, control and follow-up in accordance with the *Instruction for Compliance in the SEB Group*.

4.6 *CRO function*

The function headed by the Chief Risk Officer (CRO function) is a SEB Group-wide function which is independent from the business activities and forms part of the second line of defense. The CRO function has the overall responsibility for identifying, measuring, monitoring and controlling the risks of the SEB Group in accordance with the *Instruction for the Chief Risk Officer*.

4.7 *Group Internal Audit*

Group Internal Audit is a SEB Group-wide function that is independent from all other activities in

the SEB Group and constitutes the third line of defense. Group Internal Audit has the main responsibility to provide reliable and objective assurance to the Board and the President as concerns the effectiveness of controls, risk management and governance processes in the AML/CFT area in accordance with the *Instruction for Internal Audit in the SEB Group*.

5. Revision and approval

Group Compliance shall maintain and update the content of this Policy. Review of the content of this Policy shall be performed at least annually or more frequently if so required, and the content shall be updated as necessary or appropriate to reflect changes in AML/CFT laws and regulations as well as industry practice, or SEB's risk tolerance.

6. Non-compliance to Group Policy Requirements

6.1 *Deviation requests*

The SEB Group shall comply with all requirements in this Policy. However, specific circumstances or local requirements may warrant a deviation from this Policy.

Where there are differences between the requirements in this Policy and local laws or regulations, compliance with in-country local regulatory requirements may be requested and a deviation may be applied for where parts of the SEB Group is unable to meet a particular requirement of this Policy. Warranted deviations shall be approved by the Group FCP Committee.

6.2 *Breaches*

Non-compliance with any requirement in this Policy that has not been approved as a deviation, is considered a breach. All breaches or potential breaches of this Policy shall be reported without delay to Group Compliance as well as to the relevant and mandated group-functions within SEB's first line of defense.

Policy breaches are matters of serious concern that may place SEB at risk of violating AML/CFT laws and regulations or identify historical violations. Where a breach of this Policy is also a breach of AML/CFT laws and regulations, Group Compliance shall ensure the reporting of such matters to competent authorities, where required.

Specific and detailed requirements on mitigation plans and the tracking of actual or potential breaches shall be described in underlying instructions and procedures.

7. ML/TF Risk Management

The risk of being exposed to ML/TF varies across customers, countries, delivery channels, products, services and over time. High risk situations demand stronger controls than lower risk situations. To manage and mitigate these risks, a risk-based approach shall be applied. The guiding principle is that resources shall be directed in accordance with priorities, so that the greatest risks receive the highest attention.

SEB is committed to mitigate and manage ML/TF risks by:

- maintaining appropriate risk-based AML/CTF compliance systems and controls to execute AML/CFT risk management activities within SEB's risk tolerance;

- a strategic and systematic approach to the identification, assessment and management of ML/TF risks;

- securing capable and suitably trained resources who can fulfil their responsibilities consistently and effectively; and

- clear oversight of AML/CFT risk at management level, with clearly articulated escalation pathways and decision-making responsibilities.

7.1 *Business-wide ML/TF risk assessment*

The foundation of SEB's AML/CFT risk management is a business-wide ML/TF risk assessment, which allows SEB to identify and assess its inherent ML/TF risks and evaluate the design and operational effectiveness of mitigating controls. The business-wide ML/TF risk assessment shall at least take consideration to ML/TF risks in relation to SEB's customer base, geographies involved, products and services SEB offers, delivery channels and other relevant information.

The Group FCP Senior Manager is responsible for defining risk assessment methodology, the performance of the business-wide ML/TF risk assessment on an annual basis and updating the business-wide ML/TF risk assessment when necessary. The Group FCP Senior Manager is responsible for reporting the results of the sanctions risk assessment to the CEO and the Board as appropriate. Among other things, the results of the business-wide ML/TF risk assessment will be used to design and optimise existing controls and processes.

7.2 *Prohibited Activities*

SEB shall not keep anonymous accounts, anonymous passbooks or anonymous safe-deposit boxes.

SEB shall not enter into or continue a correspondent relationship with a shell bank. Furthermore, appropriate measures shall be taken to ensure that SEB does not engage in or continue correspondent relationships with a bank that is known to permit its accounts to be used by a shell bank.

SEB shall not accept companies having nominee shareholders (an unrelated third party officially registered on behalf of the actual shareholder) unless information on beneficial ownership and control can be obtained and ensured.

SEB shall not accept companies having shares in bearer form (physical shares owned by the current possessor of the physical document) not registered in any share register or similar since this type of arrangement obstructs the obtaining of information on beneficial ownership and thus results in an inadequate risk assessment of the Customer.

7.3 *Know Your Customer measures*

A sound Know Your Customer (KYC) program is key to prevent ML/TF. The performance of KYC measures shall enable SEB to obtain relevant and necessary information about SEB's customers, beneficial owners and associated parties, their transactions and the nature of the business activities in order to understand and mitigate ML/TF related risks during the customer on-boarding process, as well as on an ongoing basis through the duration of the customer relationship. SEB is committed to ensuring that it performs consistent and documented KYC measures to determine the customer risk level prior to establishing a business relationship or carrying out an occasional transaction or offering new products or banking services. Such KYC measures shall be aligned to and be based on the identified and assessed ML/TF risk.

The main components in the KYC process and applying customer due diligence measures are:

1. identity check and verification of identity and relevant authority rights in relation to the customer and any associated parties when acting on behalf of the customer;
2. check of ownership- and control structure and identification/verification of beneficial owner;
3. check customer and beneficial owner regarding PEP status;
4. assess and, as appropriate, obtain information on the purpose and intended nature of the business relationship;
5. check against sanction lists in accordance with the *Instruction for procedures to handle Financial Sanctions for the SEB Group* and other relevant lists;
6. assess the customer's risk profile (risk class/risk level);
7. assign relevant due diligence level taking into consideration steps 1-6;
8. apply enhanced due diligence measures (when applicable);
9. obtain Customer Adoption Committee's approval (when applicable); and
10. ongoing customer due diligence (monitoring of the business relationship and transactions and keeping the KYC-information up-to-date, correct and sufficient according to the customer's risk profile).

SEB recognises that it is responsible at all times for its ML/TF risk management and that this responsibility cannot be delegated or outsourced outside of SEB.

7.4 *Monitoring and reporting*

SEB shall perform risk-based transaction monitoring of all customers' activities and transactions in order to identify suspicious and/or deviating activity and ensure that transactions are consistent with SEB's knowledge of the customer as regards the purpose and nature of the relationship and the customer's business activities and risk profile.

The assessment of what constitutes suspicion and/or deviations shall be based on the KYC information about the customer, and the scope of the customer's business relationship, along with SEB's general knowledge of deviating or suspicious transaction patterns.

SEB shall have a transaction monitoring system for detecting suspicious activities and support the monitoring of significant changes in customers' behaviour or business profile and unusual transactions.

SEB is also committed to ensuring that all employees remain vigilant to the risks of ML/TF, and are aware of the obligation to file an internal report where they have suspicion, knowledge or reason to believe that a customer or other party may be involved in ML or TF. Procedures for internal reporting of unusual activity shall be implemented and information provided as part of the regular training provided to employees.

All alerts generated by the transaction monitoring system and reports of unusual activities filed internally shall be reviewed and if necessary, investigated and if required escalated for in-depth investigation and possible external reporting to the local Financial Intelligence Unit (FIU). Evidence and documentation of all investigations and escalations shall be retained to confirm the activities undertaken and the decision rationale.

It is prohibited to disclose to the customer concerned or to other third persons outside SEB the fact that a report has been filed to the FIU or that a ML/TF investigation is being or has been carried out.

The obligation to report to the FIU is also applicable in situations where the business relationship has been declined, or the transaction has not been processed due to suspicious circumstances.

8. Customer risk acceptance and exit

8.1 *Customer risk acceptance*

The business unit responsible for each customer, although certain tasks may be delegated and/or centralised, is responsible for the business-wide ML/TF risk associated with its customer relationships and the acceptance of the risk in accordance with SEB's ML/TF risk tolerance. Business units shall ensure that the risks are mitigated and managed appropriately at the time of on-boarding, and on an ongoing basis through the duration of the customer relationship.

The necessary approval hierarchy and criteria for approval of the customer shall be defined by the Group FCP Committee.

8.2 *Customer exit*

A business unit may determine the need to exit a relationship with a customer, or cease or limit the provision of certain products and services, if that customer or any involved party to the customer is prohibited or falls outside of the SEB Group's ML/TF risk tolerance.

Processes and procedures shall be implemented to identify the specific circumstances and activities that may indicate whether a customer is prohibited or falls outside of the SEB Group's ML/TF risk tolerance. If it is determined that an existing customer poses an unacceptable ML/TF risk, and mitigating controls cannot be implemented, the necessary governance for customer risk approval shall be followed. The relevant business unit is responsible for ensuring that the rationale for any customer exit in relation to ML/TF risk is documented in full, and for ensuring that all customer exit execution activities are completed, although certain tasks may be delegated and/or centralised.

If a customer relationship is exited, appropriate measures to prevent the re-entry of the customer to any part of the SEB Group shall be implemented in accordance with the requirements defined in the *Instruction for procedures against Money Laundering and Terrorist Financing for the SEB Group* or accompanying procedures.

9. Requests from law enforcement and competent authorities

The SEB Group is fully committed to cooperating with requests for information from law enforcement or competent authorities in connection with ML/TF investigations, while ensuring that responses are consistent with bank secrecy or other relevant laws.

10. Monitoring and testing

SEB shall conduct monitoring and testing through its established three lines of defence.

Divisions, business units and the relevant functions are responsible for implementing procedures that include regularly scheduled monitoring and testing of the quality and effectiveness of ML/TF processes and controls. This includes testing that these processes and controls comply with this Policy and the *Instruction for procedures against Money Laundering and Terrorist Financing for the SEB Group*, and provide attestation, as required.

11. Management information

For management to maintain effective oversight of ML/TF risk management activities within SEB, the SEB Group shall have processes in place that provide for accurate and timely management information reporting in order to monitor the level of ML/TF risk and the effectiveness of AML/CFT compliance measures. Management information reporting should enable the demonstration of trends and emerging risks as well as any necessary remedial action.

The relevant parts of the first and second line of defence shall ensure for and are required to provide the necessary management information and escalate issues, including risk reporting, in line with SEB's governance and reporting model without delay.

12. Record keeping

All ML/TF related records shall be retained electronically and for the period of five years following the termination of a customer relationship or performance of an occasional transaction, taking into account any local requirements that may specify an alternative format, a longer time period or prohibit information from being held altogether due to for example data protection regulations or similar.

ML/TF related records shall be legible, of good quality, accessible and provide necessary audit trails for examination by Group Internal Audit, Group Compliance or external examiners.

The requirements for record keeping ensuring a consistent approach to record keeping within the

SEB Group that allow for taking into account local requirements due to for example data protection legislation or bank secrecy laws, shall be defined in the *Instruction for procedures against Money Laundering and Terrorist Financing for the SEB Group* or accompanying instructions and procedures. Divisions, business units and the relevant functions are responsible for ensuring record keeping in line with the defined requirements and any local requirements.

13. Confidentiality, data protection and bank secrecy

Implementation of this Policy should always consider adherence to relevant and applicable confidentiality requirements, data protection laws and regulations, including any such local laws and regulations on data privacy, information security and bank secrecy.

14. Information sharing

In order to understand its potential ML/TF risk exposure and risks of the customer base, the SEB Group shall share relevant information for AML/CFT purposes, There shall be routines for the processing of personal data and information sharing within the SEB Group in accordance with GDPR, applicable local legislation and the *Instruction for procedures against Money Laundering and Terrorist Financing for the SEB Group* and further described in accompanying instructions and procedures.

15. Training

For the SEB Group to manage its ML/TF risks effectively, all relevant employees, contractors and others who similarly participate in activities, and perform tasks of importance, with regards to preventing SEB from being used for money laundering or terrorist financing, shall undertake mandatory awareness training and role specific training where appropriate.

The minimum requirement for the training strategy shall be defined in the *Instruction for procedures against Money Laundering and Terrorist Financing for the SEB Group* and further described in accompanying instructions and procedures.

16. Protection of staff and whistle blowing

SEB shall take all appropriate measures to protect employees, representatives and contractors who internally or externally to the FIU, report suspicious activity from being exposed to threats, retaliatory or hostile action. SEB shall also secure that employees, representatives and contractors who internally or externally to the FIU, report suspicious activity are protected from adverse or discriminatory employment actions.

The SEB Group has implemented a Whistleblowing process for reporting irregularities. Any employee, representative and contractor in a corresponding position discovering possible unethical or unlawful behaviour or breaches of the requirements under this Instruction may report such irregularities in line with the process as described in the *SEB Code of Conduct* and on the Intranet.

17. Suitability assessment

SEB shall establish relevant processes and routines in order to secure that all employees and contractors that conduct tasks of significance to combat ML/TF have appropriate knowledge of AML/CFT and otherwise are assessed as suitable for their tasks.

18. Outsourcing

Divisions, business areas, business units and other relevant functions may outsource certain ML/TF risk management activities, which they are responsible for. The divisions, business areas, business units and other relevant functions that has outsourced ML/TF risk management activities remains responsible for ensuring that these activities are undertaken in compliance with this Policy. The responsibility for the ownership and management of ML/TF risks cannot be outsourced.