Extract from the Instruction for procedures against Money Laundering and Terrorist Financing and for handling of Financial Sanctions for the SEB Group

derived from the Instruction for the President and Chief Executive Officer

adopted by the President and Chief Executive Officer of
Skandinaviska Enskilda Banken AB (publ)
on 18 January 2021

Group Compliance

Security Class 1/External

1. General

1.1. The SEB Group shall, as part of its normal business conduct, combat Money Laundering and Terrorist Financing. 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.

1.2. The risk of being exposed to Money Laundering and Terrorist Financing 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.

1.3. Furthermore, SEB is committed to complying with the sanctions laws and regulations of the European Union, the United Nations and the United States (OFAC), as well as other applicable sanctions laws and regulations in the jurisdictions in which SEB operates, subject to the primacy of local laws and regulations.

1.4. This Instruction shall apply to the SEB Group. Branches and subsidiaries shall take necessary steps to implement the Instruction that constitutes a mandatory minimum standard. This means that deviation from the principles only is acceptable if a) the deviation means a stricter procedure and is required by local regulation, or b) in situations where local regulation prohibits application of the minimum standard.

2. The SEB Group's AML and FS Governance Model

2.1. The SEB Group's AML and FS (Financial Sanctions) Governance Model shall be based on a three-line of defense approach.

First line responsibility rests within divisions, business areas and business units, subsidiaries, branches and affiliated companies. The first line is responsible for the implementation of AML/CFT and FS procedures and controls, as well as for a comprehensive ML/TF and FS Risk Assessment and risk management.

SEB shall appoint a Group AML Senior Manager, who shall be a member of the Group Executive Committee (GEC) and appointed by the CEO. The Group AML Senior Manager shall have the overall responsibility for the implementation of AML/CFT and FS requirements in the SEB Group.

2.2. Second line responsibility rests with Group Compliance and Group Risk. The Head of Group Compliance has also the central functional responsibility, including inter alia the responsibility to report Suspicious Activity Reports to the Finance Intelligence Unit.

2.3. Third line responsibility rests with Group Internal Audit having an independent responsibility to review and evaluate the SEB Group's AML/CFT and FS governance, instructions, procedures and control processes appropriateness and efficiency and to review and evaluate the SEB Group's risk management in relation to its ML/TF and FS Risk Assessment.

3. Management of ML/TF and FS Risks

Management of ML/TF Risks

3.1. In order to understand how SEB can be used for ML/TF purposes and manage risks in a structured and efficient way, a ML/TF risk assessment process shall be in place to help SEB set sufficient and suitable working routines and processes that comprise appropriate, adequate and proportionate mitigating measures to reduce the identified risks. The 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.

3.2. The ML/TF Risk Assessment shall be documented and conducted at least annually on a Group, divisional, local and business unit level.

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

3.4. 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.

3.5. 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.

3.6. 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.

Management of FS Risks

3.7. SEB shall conduct a FS Risk Assessment that shall provide the foundation to an ongoing understanding and effective management of FS risks.

3.8. As a minimum Customers, Beneficial Owners, Associated Parties who are acting on behalf of the Customer in a transaction or agreement/business relationship and international transactions shall be screened against the sanctions list issued by the European Union, the United Nations and the United States

(OFAC). In addition, SEB shall screen against other sanctions list that apply to SEB's operation in a particular jurisdiction.

3.9. Business activities, including commencing or continuing customer relationships or providing products or services or facilitating transactions, are prohibited if SEB believes that the activity may violate applicable FS regulations or SEB's internal FS requirements.

Furthermore, SEB shall restrict from business activity involving, directly or indirectly, selective or targeted sanctions programs. These sanctions apply restrictions on some types of products or services or target certain industry sectors or governments.

3.10. SEB shall block or reject transactions where SEB is required to do so under applicable sanctions laws or regulations or SEB's internal FS requirements. Transactions may also be returned by SEB where they fall outside of SEB's risk appetite in relation to sanctions.

Any breach of sanctions regimes must be reported to the competent authorities in accordance with local laws or regulations.

3.11. SEB may agree to process certain transactions, in its sole discretion, such as those which relate to humanitarian aid or which are otherwise permitted by a license from an appropriate authority. These transactions will be considered on a case-by-case basis and must be approved prior to the transaction taking place.

4. Know Your Customer (KYC)

4.1. A sound KYC program is the best method to prevent ML and TF, the basis of a professional relationship with Customers, and an important tool to apply an appropriate level of customer due diligence measures.

4.2. 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 party 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 and other relevant lists;
6. assess the Customer's risk profile;
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).

4.3. If there are gaps in the KYC Information, or if ambiguity or uncertainty occurs in relation to the information provided by a Customer, additional questions shall be asked or additional documentation requested. Where the identity of the Customer cannot be verified without doubt, or information on beneficial ownership and control as well as purpose and intended nature of the business relationship cannot be obtained, a business relationship shall not be entered into, nor shall one-off transactions or transactions initiated by the Customer be executed.

4.4. Enhanced due diligence measures will be applied to Customers that in any situation which by its nature indicates a higher risk. The following circumstances shall always be assessed as a high risk and lead to enhanced due diligence measures when onboarding the Customer and on an ongoing basis (unless local regulation stipulate otherwise):

1. the business relationship or transactions involve a high risk third country identified by the European Commission;
2. the Customer or Beneficial Owner is a PEP or Family Member or Close Associate of a PEP;
3. Correspondent Relationships involving the execution of payments with a credit- or financial institution domiciled outside the EEA;
4. the Customer, following an evaluation based on the ML/TF Risk Assessment foundation, is seen as representing a high risk, e.g. due to customer-, country-, product and services-, delivery channel and/or combination risks; and
5. if the customer's behaviour or other circumstances indicates high risk.

5 Monitoring and reporting

5.1. Customers' activities and transactions shall, based on a risk-based approach, be monitored in order to identify suspicious activity. The assessment of what constitutes suspicion shall be based on the information about the Customer obtained by the employee handling the matter, and the scope of the Customer's business relationship, along with SEB's general knowledge of deviating or suspicious transaction patterns.

5.2. 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.

5.3. It is prohibited to disclose to the Customer concerned or to other third persons outside SEB the fact that a SAR has been filed or that a ML/TF investigation is being or may be carried out.

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

Protection of employees and whistle blowing

5.5. SEB must 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.

5.6. The SEB Group has implemented a Whistleblowing process for reporting irregularities. Any employee or person 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.

6. Recordkeeping, Data Sharing and Data Protection

6.1. All KYC information shall be kept for a period of at least five years after the business relationship with the Customer has ended or, in the case of one-off transactions, after the execution of the transaction, unless a longer retention period is required under applicable local law.

6.2. Sharing of information within the SEB Group is allowed and the same data protection level shall be ensured. Information on suspicions that funds are the proceeds of criminal activity or are related to terrorist financing reported to the FIU shall be shared within the SEB Group, unless otherwise instructed by the applicable FIU. Local regulation may apply.

6.3. The processing of personal data maintained in the process under this Instruction shall be made for the purposes of prevention of ML and TF and shall not be further processed in a way that is incompatible with those purposes. The SEB Group internal instructions in relation to confidentiality and data protection and information security shall always apply.

Upon expiry of the retention periods it shall be ensured that personal data is deleted, unless otherwise provided for by applicable local law.

7. Suitability assessment

7.1. 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.

8. Training

8.1. All employees and relevant contractors within the SEB Group shall have general understanding and awareness of AML and CFT requirements and ML/TF risks. For this reason, all employees and relevant contractors shall be required to pass a group common training programme with recurring intervals.

8.2. All employees and relevant contractors dealing with Customer related matters shall be provided with adequate training, comprising, amongst other things, local legislation and other external regulations regarding actions to be taken against ML and TF and the internal instructions that apply in addition thereto. The training shall be tailored according to identified risks in the ML/TF Risk Assessment.

9. Outsourcing

9.1. The measures to prevent ML and TF, described in this Instruction, are of material significance to SEB. Any part of the SEB Group that considers commissioning another party to perform AML/CFT tasks and functions shall apply relevant principles and instructions in the Outsourcing Instruction for the SEB Group, as well as applicable local regulations.