SpareBank 1 SR-Bank ASA
Group Guidelines for AML and Sanctions

1. GROUP GUIDELINES – GENERAL PRINCIPLES

The SpareBank 1 SR-Bank ASA Group (SpareBank 1 SR-Bank or the Group) is aware of its social responsibility to combat economic crime, money laundering from the proceeds from crime and financing terrorist activities. The authorities, customers and competitors must have confidence in the professionalism and integrity of SpareBank 1 SR-Bank. The Group will comply with laws and regulations that apply to our corporate operations through vigilance at all levels in the organization.

SpareBank 1 SR-Bank shall strive for the lowest possible risk of money laundering and terror financing. This implies that the Group shall maintain a constructive approach to the interpretation of laws and regulations, a high level of structural compliance, good system support and strive for continuous improvement in how we deal with money laundering and terror financing.

The Group Guidelines are available on the bank's website, in Norwegian and English. The updated Wolfsberg Group AML Form is available on the bank's website.

Money laundering and terror financing risk is part of the Group's ICAAP assessment.

In accordance with the Group's quality assurance system, this document is considered the Group's policy for all aspects of AML.

2. PURPOSE AND SCOPE

The purpose of SpareBank 1 SR-Bank's Group Guidelines for AML and Sanctions is to provide guidelines and principles for establishing, implementing, improving and monitoring compliance to the Norwegian Money Laundering Act and other rules for imposing sanctions. The Guidelines will clarify the roles and responsibilities of this work when it comes to manual, systematic and automated routines.

The document is intended to provide a general description of measures implemented at a corporate level, including guidelines and principles for our company's management and control environment and how we organize the company to ensure compliance with legal requirements.

The Group AML and Sanctions Guidelines apply to the entire SpareBank 1 SR-Bank Group, including all business areas, organizational units, subsidiaries, employees and managers. Our subsidiaries – Eiendomsmegler 1 SR Eiendom AS, SpareBank1 SR-Bank Forretningspartner AS, SR-Boligkreditt AS and

Monio AS are obligated to report any suspicious transactions to the Financial Supervisory Authority of Norway, pursuant to the Money Laundering Regulations.

3. LEGAL AND REGULATORY REQUIREMENTS, DEFINITIONS AND FRAMEWORK

3.1 Legal and regulatory requirements

SpareBank 1 SR-Bank is obligated to report suspicious transactions pursuant to the Money Laundering Act and its Regulations, and to comply with the rules for sanctioning in Norway. Guidance from the regulatory authorities forms part of the regulatory requirements. The Financial Supervisory Authority of Norway (www.finanstilsynet.no) is authorised to audit and inspect SpareBank 1 SR-Bank activities.

3.2 Definition of money laundering, terror financing and sanctions

The Group Guidelines utilise international terminology for money laundering and terror financing: Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF). Under Norwegian law, money laundering is defined as a self-laundering; see Section 337 of the Penal Code. Money laundering exists when the purpose is to safeguard the proceeds of a criminal act. In order for the proceeds to be used by the perpetrator, they must be integrated into the legal economy. The purpose of money laundering is thus to get proceeds to appear as if they were acquired in a legal manner, i.e., to hide their illicit origin.

Terror financing exists when financial support is provided, or money is collected for persons or groups who intend to use the money to commit acts of terrorism; see Sections 131–136a of the Norwegian Penal Code.

Sanctions are defined as "non-military measures in the form of prohibitions against or limitations on economic or other interactions with countries or political movements"; see Section 1 of the Norwegian Sanctions Act.

3.3 Framework for AML and Sanctions

SpareBank 1 SR-Bank shall develop and maintain an internal framework for addressing money laundering and terror financing issues and sanctions. The framework will build on the most recent risk analysis of measures to combat money laundering and terror financing as well as safeguarding the requirements for the sanctioning system. The framework is to be adapted to the individual business units, and subsidiaries must adapt the framework to fit their business.

The framework should ensure that the Group complies with the basic requirements and standards in the area, as well as contributing to uniform implementation throughout the Group. The framework sets the overall standards and principles for Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF), which is integrated in the Group's business processes.

In addition to the current work processes described in the bank’s quality system, the bank’s framework contains the following documents, which are dated and approved at the correct administrative level:

1. Company-wide risk assessment
2. Group Guidelines for AML and Sanctions
3. Primary requirements
4. Customer monitoring
5. Electronic monitoring
6. Processing personal data
7. Training
8. Distribution AML
9. Case handling routines for investigating and reporting AML
10. Sanctions legislation
11. Internal controls

Framework for subsidiaries primarily consisting of:

1. Company-wide risk assessment
2. Routines and work processes
3. Service level agreements (SLA)

If a violation of regulatory requirements or internal rules is identified, the incident must be recorded in the incidents database of the company that is obligated to report such matters. The Group has established an internal alert system that is used for all matters relating to a possible violation of the money laundering rules. The solution also complies with requirements for anonymity of alerts.

4. ROLES AND RESPONSIBILITIES

4.1 Board of directors

The board has overall responsibility for AML issues at the Group and shall ensure that applicable laws and regulations are complied with. The board is responsible for decisions regarding the Group Guidelines for AML and Sanctions; see Section 8(4) of the Money Laundering Act. The board shall review and approve the Group's money laundering and terror financing risk analysis at least once a year.

4.2 Group managing director

The managing director shall make certain the Group has a satisfactory framework and have effective systems and controls in place in accordance with the guidelines set by the board of directors. The managing director shall ensure that this matter receives adequate attention and necessary resources.

4.3 Money laundering officer

The board has appointed a Group Money Laundering Reporting Officer (GMRLO), who is assigned the task of ensuring framework compliance at an executive level. The GMRLO reports directly to the Group managing director.

The GMRLO has responsibility for ensuring adequate follow-up of anti-money laundering and terror financing routines and making sure the Group's policies, procedures and framework are sufficiently

supported by the board of directors and executive management. The GMRLO monitors our systems to make sure the routines are executed in a satisfactory manner.

4.4 Head of AML Section – Money Laundering Reporting Officer (MRLO)

The head of the AML Section/Money Laundering Reporting Officer has been delegated strategic and operational responsibility for AML work at the Group. The delegation includes responsibility for preparing the AML strategy and operationalising the strategy, investigating and reporting, developing digital monitoring systems and providing training in these matters, or ensuring learning and training of staff in these matters. This is done to strengthen knowledge of the risks within our business culture and to ensure good processes.

4.5 AML Section

The AML Section is led by the head of the AML Section/Money Laundering Reporting Officer, who reports directly to the GMRLO. The AML Section shall have satisfactory staffing at all times to carry out the tasks and responsibilities imposed on the section where level of expertise and capacity are concerned. The Money Laundering Reporting Officer has formal responsibility for delegating tasks to AML Section employees who are responsible for investigating and reporting suspicious transactions to Økokrim (the National Authority for Investigation and Prosecution of Economic and Environmental Crime).

4.6 Compliance officer

The Group managing director for Compliance is the compliance officer, cf. the Money Laundering Act §35. The compliance officer shall maintain a control function with a sufficient degree of independence to the work otherwise carried out in the organization. The compliance officer must ensure that independent controls and assessments to ensure that the organization complies with the Money Laundering Act are executed, and that the measures implemented to remedy identified deficiencies are effective.

4.7 Business divisions and subsidiaries

The Group managing director for SME & agriculture, for the Corporate Market, for the Retail Market and for the Capital Market are each individually responsible for the implementation and operationalisation of the guidelines, routines, and procedures at their respective business divisions. Each business division shall appoint its own AML manager. All business divisions should consider whether there is a need to establish additional support and control functions in their division. The business divisions shall also contribute by preparing a risk assessment of their own business division, where the main features are included in the group's business-oriented risk assessment.

At the subsidiaries with a reporting obligation, the respective boards are responsible for ensuring implementation of the guidelines in their companies' routines and work processes. The subsidiaries report quarterly to the group board and shall prepare risk assessments that are suited for their individual activities each year, which are reviewed by their respective boards. A money laundering officer shall be

appointed at each company, who is delegated the responsibility of upholding the AML requirements for each company.

Every SpareBank 1 SR-Bank manager shall be responsible for implementing the AML processes in his or her area of responsibility and ensure compliance to applicable external and internal rules and regulations. Execution shall have a risk-based approach and ensure that the processes are sufficiently effective through ownership and good documentation.

All employees of parts of the Group with a reporting obligation shall have read and understood their specific obligations pursuant to money laundering regulations. Employees should be able to recognise suspicious transactions and be familiar with internal procedures that apply to dealing with such transactions. Training in these matters is obligatory for all employees. All our employees are personally responsible for compliance with the Group's routines and guidelines when performing their work tasks.

4.8 AML and Sanctions Forum

The Group has established an AML and Sanctions Forum as a group-wide forum that provides advice and guidance for SpareBank 1 SR-Bank compliance with international sanctions and regulations to combat money laundering and terror financing. The forum consists of the GMRLO, the Group managing director for Compliance, the AML/Money Laundering Reporting Officer, representatives from the AML Section, representatives from relevant support and development divisions and executives from the business divisions. The forum will meet quarterly and as needed. Representatives from the subsidiaries will meet twice a year in a separate forum, more often if necessary.

4.9 Internal controls

SpareBank 1 SR-Bank builds its framework for internal controls on the COSO Model (Committee of Sponsoring Organizations of the Treadway Commission); monitoring and compliance are done according to the three lines of defence. Internal Control means all measures that are designed to ensure compliance with the AML requirements, including inspection and control functions on three lines of defence (first, second and third) and the implementation of routines and systems, competence and resources.

The AML Section and the business divisions are part of the first line of defence. The business divisions are responsible for managing, control checks and compliance in their own business areas and shall be liable for and handle the operative risks. Each business area and support area shall make certain all employees at all levels have the right skills, that relevant risk assessments are carried out and that AML, CTF and sanctions work is monitored and evaluated regularly.

The second line of defence is an independent function which monitors and follows up on the governance and internal controls done by operational management. The Compliance team has a special responsibility regarding compliance according to the Money Laundering Act and reports to executive management and the board regarding compliance.

The third line of defence is an external and independent audit of our internal processes which examines and evaluates the Group's overall governance and internal controls for all areas related to money laundering. The internal audit is done independently of the administration and reports directly to the board.

In EiendomsMegler 1 SR Eiendom AS the responsibility for anti-money-laundering is organized in the second line of defense within a role that reports directly to the board of directors and the CEO. The first line of defense is executed by subject managers in each section. Controls in the second line of defense are executed by resources in the subject division, led by the anti-money-laundering officer.

In SpareBank 1 SR-Bank ForretningsPartner AS the anti-money-laundering officer is organized as the subject manager in the company and reports directly to the board of directors and CEO. The anti-money-laundering officer is involved in the operational AML work, including internal controls. Based on the inherent risk of the company, the specter of products and services they provide and overall internal control measures, designating a compliance officer is deemed unnecessary.

In Monio AS the anti-money-laundering officer is organized in the company's management group and reports directly to the board of directors and CEO. The company considers that the business is of such nature and scope that is does not trigger the requirements for a compliance officer, according to section 35, second paragraph, of the Money Laundering Act.

Every subsidiary has established a third line of defense, which is handled by independent internal auditors.

5. PRINCIPLES FOR MANAGING AND CONTROLLING MONEY LAUNDERING AND TERROR FINANCING

5.1 Risk-based approach

Working with money laundering and terror financing shall be based on a risk-based approach. An annual risk assessment shall be prepared for the Group as a whole, including the business divisions, and for each subsidiary that has a reporting obligation. The risk assessment shall build on the national risk assessment prepared by the Ministry of Justice and Public Security, the Financial Supervisory Authority's risk assessment and other national and international relevant sources. Crucial to risk assessment and compliance with money-laundering legislation are clear guidelines from the Norwegian Financial Supervisory Authority that risk should be managed and should not be inconsistent. As part of the risk assessment, the Group shall:

- Identify the risks for money laundering and terror financing where such things as Products and services / Customer segment / transaction / geographic area / distribution channels / bank measures are concerned.
- Identify and implement risk-reducing measures, as well as updating the routines.
- Identify the risk of a breach of the sanction's regulations with a focus on whether there are customer relationships or transactions in breach of the sanctions regulations.

- Ensure adequate training and commitment within the Group.
- Ongoing evaluation of the efficiency of risk-reducing measures to hinder money laundering and terror financing.

5.2 Training

All employees in the Group, including board members at the parent company and subsidiaries, shall complete AML training according to a Training Plan prepared by the AML Section in collaboration with the business units and the subsidiaries. Training also has a risk-based approach and is tailored to the role and responsibility of the individual employee/elected representative. The requirements for training also apply to temporary employees (temps, substitutes, student employees etc.).

5.3 Know Your Customer

At SpareBank 1 SR-Bank, our processes must be set up to counteract anonymity and strive for transparency, with the goal of preventing money laundering and terror financing. This is done by:

- **Confirming a customer's identity.** The customer's identity shall be verified and documented every time a new customer relationship is established.
- **Knowing the purpose and nature of a customer relationship:** Before a customer relationship can be established, the bank will have collected and evaluated the information provided by the customer about the purpose and nature of his or her activities.
- **Identifying and registering the real rightsholders and politically exposed persons (PEP):** All customers shall answer the questions regarding real rightsholders and politically exposed persons. Regarding high-risk customers with complex ownership structures, further investigations will be needed to verify the collected information, including documenting these.
- **Risk classification of customer relationships:** Customer relationships are classified by risk, based on information about e.g., the purpose of the customer relationship, usage patterns for products/services/transactions, type of customer and type of owner.
- **Register and archive information about the customer and the customer relationship:** All activities concerning customer control checks shall be documented and archived according to current applicable rules for archiving obligations.

5.4 Control mechanisms

5.4.1 Customer due diligence

Customer due diligence is done before establishing a customer relationship and before agreements and transactions are used/executed.

Confirming the customer's identity by physically meeting an employee at the bank shall be the main rule. If the customer cannot meet in person, special measures shall be established to confirm the customer's identity. BankID issued by another bank is considered a legitimate identification.

Both when the customer is a natural person and a legal person, the bank must determine whether any other real rightsholders exist, in addition to the customer himself/herself.

5.4.2 Level of customer due diligence and expanded control

Customer due diligence shall be suited to the organization and information about the customer. Different levels for control checks shall be used, based on the customer's risk classification. Special routines and criteria shall be established for the different risk classes, and this shall be based on the latest risk assessment.

If the customer's risk level is high, the due diligence must be expanded to an adequate level. Enhanced customer due diligence can involve:

- Exploring the nature and purpose of the customer relationship in more detail.
- Documenting the source or origin of the funds and/or assets/wealth.
- Documenting key financial figures, including turnover.
- Documenting business connections.
- Documentation that confirms the identity of real rightsholders.
- Justifications for a complex company structure.
- Documenting the customer's relationship to Norway and need for a bank account and financial activities, if the customer is not domiciled here.

Customers who are Politically Exposed Persons (PEP) are always considered to have a higher risk level which requires an enhanced due diligence. The same applies to a PEP who has roles or is a Real Rightsholder (RRH) as a legal person. Establishing or maintaining a customer relationship where a PEP is involved must be approved by a manager with special authorisation to do so. The source or origin of the funds or wealth shall always be documented when they form part of the customer relationship. A specific evaluation is done on the documentation collected in an enhanced due diligence case, to make sure it is adequate, also to make sure the customer can be offered all our products/services. This evaluation shall be documented.

Regarding customer relationships and transactions involving states included in the first and second section of the Money Laundering Act §4-10, enhanced due diligence must be carried out at a minimum, according to the aforementioned provisions.

5.4.3 Ongoing customer due diligences

SpareBank 1 SR-Bank shall conduct ongoing verification of all customer relationships.

Information about customers and customer relationships shall be updated on a regular basis using public sources and supplemented where necessary by contacting the customers as needed (updating customer information).

Information about the customer and the customer relationship shall be collected on a regular basis. Information on high-risk customers shall be updated annually. For all other customers, routines shall be in place to frequently update customer information, based on the existing risk scenario.

Regarding the sale of additional products or services in previously established relationships, the customer information shall be reviewed, revised and updated as needed.

5.4.4 Customer due diligence for distributors and agents

Even though the due diligence is done by our agents/distributors, SpareBank 1 SR-Bank is still ultimately responsible for the verification and control checks. When this is the case, employ an underlying distribution agreement and/or other relevant steering documents that list the quality requirements for the due diligence processes.

5.4.5 Customer due diligence for correspondent and respondent bank connections

SpareBank 1 SR-Bank has decided not to act as a correspondent in correspondent connections for other banks and payment providers, but only be the respondent.

When entering into respondent banking agreements, specific risk assessments and due diligence investigations must be conducted. Special routines have been established for this. Respondent banking agreements shall not be established with empty banking companies, or with banks in defined high-risk countries, and sufficient investigations must be carried out to ensure this.

As a general rule, no agreements are to be made with an institution from states outside the EEA that function as respondent institutions. The following requirements are set for such relationships:

- Sufficient information must be acquired about the respondent institution to understand the nature and reputation of the enterprise or company and ensuring the quality of supervision.
- The respondent institution's measures to combat money laundering and terror financing shall be evaluated.
- The Group managing director for Finance (CFO) must sign the formal approval before establishing the relationship.
- Before opening the settlement account, the Bank needs to make sure that the respondent institution:
    - has confirmed the identity of and regularly monitors customers with direct access to the accounts in the correspondent institution, and
    - upon request, can provide relevant information to the correspondent institution about customer due diligences and regular customer monitoring.

5.5 Rejection of customers, blocking and closing customer relationships

The customer relationship will not be established if a customer fails to cooperate in the verification, including any obligatory expanded verifications.

Similarly, as a general rule, the customer relationships will be terminated or blocked if a customer fails to cooperate with the verification in an existing customer relationship.

5.6 Investigating and reporting

An investigation shall be launched whenever the bank suspects a transaction is associated with funds from money laundering or terror financing. An investigation will always be launched if conditions are discovered that deviate from our knowledge of the customer and the purpose and intended nature of the customer relationship.

The following conditions and transactions shall always be investigated:

- The transaction seems to lack a legitimate objective.
- The transaction is especially large or complex.
- The transaction is unusual for the customer's known commercial or personal pattern of transactions.
- The transaction is done to or from a person in a country or area that does not have satisfactory measures in place to combat money laundering and terror financing.
- The transaction is unusual, for any other reason.

If the investigations fail to refute the suspicion, the matter will be reported to the National Authority for Investigation and Prosecution of Economic and Environmental Crime, without delay.

Generally, the transaction shall not be executed before the National Authority for Investigation and Prosecution of Economic and Environmental Crime has been informed. If stopping the transaction is not possible, or if stopping the transaction would hinder the investigation of a person that might benefit from a suspicious transaction, the National Authority for Investigation and Prosecution of Economic and Environmental Crime must be notified immediately after the transaction has been carried out.

5.7 Transaction monitoring

All customer accounts are subject to regular monitoring (either manual or digital) to uncover suspicious transactions. Digital monitoring includes all systems for transactions to or from the bank's customers. Special routines are to be prepared for systems for digital monitoring, and the use of these shall be evaluated and documented regularly. If automated digital monitoring is interrupted, measures must be implemented to identify suspicious transactions, such as checking the Transaction Register in the Group's data warehouse.

The bank's digital monitoring system shall identify suspicious transactions and customer behaviour based on criteria/rules from the Group's risk analyses. In addition to daily transaction monitoring, the bank (along with the other banks in Alliansebankene) has developed a machine learning model that flags suspicious customer behaviour on a monthly basis.

All transactions are monitored daily, and any matching entry is screened against international sanctions lists (UN, EU and OFAC lists for foreign transactions). Transactions in foreign countries should be screened before a transaction is carried out. New customers should be screened against the Sanctions List and PEP List before establishing a customer relationship. The Customer Register should be screened against the sanctions lists and against the PEP lists, once a month.

It is a prioritized work in the bank to be up to date in handling suspicious relationship and the bank must report any arrears beyond what the framework allows in the quarterly report that goes to the group's board.

Operational disruptions or errors that significantly reduce the functionality of the bank's digital monitoring equipment shall be reported to the Financial Supervisory Authority without unnecessary delay.

6. PROHIBITED ACTIVITIES

SpareBank 1 SR-Bank does not accept:

- Assets or funds that are known or suspected to be the proceeds of criminal activity/actions.
- The establishment/maintenance of business relationships with individuals or legal entities found on sanctions lists, known or suspected to be associated with terrorist activities, criminal organizations or members of such. The Group follows the updated guidelines for freezing or blocking funds as of 30.06.2023, set by the the Ministry of Foreign Affairs.
- Establishing customer relationships with empty banking entities; see Section 20 of the Money Laundering Act, or companies which are known to permit their accounts to be used by empty banking entities.
- Establishing customer relationships or executing transactions with companies without significant assets and/or activity ("empty companies"). The bank may deviate from these requirements for Norwegian companies, yet only following an enhanceddue diligence which is carried out according to established routines.
- Entering into customer relationships with customers from sanctioned countries.
- Establishing or maintaining relationships with individuals or legal entities where the risk of tax evasion is considered significant.
- Entering into relationships with customers that operate in the following industries:
    - development, testing, production, storage or transportation of controversial weapons or components exclusively considered controversial weapons, including cluster bombs, anti-personnel mines, nuclear weapons, chemical weapons and biological weapons.
    - companies that produce tobacco products or components expressly intended for such products.
    - companies that produce pornographic material.
    - illegal gambling.
    - money service businesses (MSB) that do not have permission to run a business in Norway.
    - suppliers of exchange services and storage services for virtual currency that are not registered with the Financial Supervisory Authority of Norway.

7. SANCTIONS

SpareBank 1 SR-Bank shall comply with sanctions from Norway, EU, UN, United States and UK. Activities that are subject to sanctions from the named authorities or official agencies are prohibited.

SpareBank 1 SR-Bank shall comply with the freezing obligation and the rules for blocking/earmarking funds from national and international authorities.

The customers and transactions shall be screened regularly by checking the sanctions lists (UN, EU and OFAC). The Money laundering officer for the Group or his authorised representative are responsible for freezing funds and reporting.

A separate risk assessment of the sanctions regulations is prepared. The group must have a conservative approach to handling the sanctions regulations. Selected risk appetite is further described in the risk assessment.

8. REPORTING

The Group's employees shall report all suspicious transactions to the AML Section. Suspicious transactions where the suspicion is not disproved after the investigation will be reported to ØKOKRIM/FIU (www.okokrim.no). Subsidiary companies with a reporting obligation will report such matters directly to the National Authority for Investigation and Prosecution of Economic and Environmental Crime/FIU.

9. CONFIDENTIALITY

Personal data is processed as confidential and according to current laws and regulations.