Luminor

LUMINOR BANK ANTI-MONEY LAUNDERING AND SANCTIONS COMPLIANCE POLICY PRINCIPLES

February 2023

GENERAL PRINCIPLES

As a bank, we are firmly committed to adhering regulatory, ethical, and social responsibilities and ensuring that our products, services, or channels are not used for purposes of money laundering, tax and sanctions evasion, terrorism financing and proliferation of weapons of mass destruction.

We take proportionate measures and have adopted and implemented set of policies and standards outlining the principles and processes for combating money laundering, terrorism financing, sanctions evasion and proliferation of weapons of mass destruction. Our policies and standards are developed in compliance with the laws and regulations of the countries where we are operating (Estonia, Latvia, Lithuania), international legal acts and best practices. Our policies and standards are applicable to the Luminor Bank AS and all our subsidiaries, approved by our Supervisory Council and reviewed annually.

We foster compliance culture, and we expect our clients, partners, vendors, suppliers and other third parties to comply with all applicable laws and regulations concerning anti-money laundering, terrorism financing, proliferation of weapons of mass destruction and implementation of sanctions.

MAIN PRINCIPLES

Risk strategy

Our risk strategy is based on the core business principle to predominantly serve Customers who are residents of Estonia, Latvia and/or Lithuania, and Customers with a strong personal or business connection to the Baltic countries. To support the strategy, we have implemented and maintain properly functioning risk management framework which is composed of the policy, risk appetite (absolute and conditional risk limitations), standards and operational requirements detailed in lower-level procedures. Risks are managed and mitigated by applying a risk-based approach, which allows us to apply proportionate controls in relation to the degree of risk.

We make exceptions from our risk appetite only following internal framework where absolute limitations are not in breach and including seniority in decision making. We have set limits to continuously monitor our risk appetite and we inform our Management Bodies on them regularly.

Roles and responsibilities

We implement three lines of defense model to ensure effective governance and oversight of money laundering, terrorism financing, proliferation of weapons of mass destruction and sanctions risks. We have introduced clear roles and responsibilities in respective areas with defined accountability that cannot be delegated. We perform suitability assessment of employees who are accountable for preventing us from being used in money laundering and sanctions evasion schemes. We invest and train all employees to be able to recognize suspicious activity and act respectively.

Knowing your customers and due diligence

To prevent our services, products and/or infrastructure from being misused we have a robust and adequate know-your-customer (KYC) programme in place. KYC measures are applied to properly identify the Customer, the beneficial owner(s), to understand the purpose and intended nature of the business relationship, as well as verify the information from the reliable and independent sources. The extent of the knowledge about the Customer corresponds with the risks associated with the Customer. The higher the risk, the more risk mitigation measures are applied to understand the Customer and its activities. We conduct ongoing due diligence on Customers' relationship. For Customers with identified red flags we perform ongoing enhanced due diligence more often. In addition, we screen our Customers against PEP (politically exposed person) lists and adverse media to identify related risks without delay. We protect all the information provided by Customers concerning their data and activities.

Transaction monitoring and reporting

We perform risk-based transaction monitoring on all transactions performed by our Customers. We have measures in place allowing automated real-time monitoring of transactions and measures enabling transactions to be analysed in later stage. Measures taken to monitor the Customers and transactions are risk-based, considering the Customer's risk profile, size, nature, scale, degree of complexity and inherent risks of the activities and services provided by the us. We report all suspicious transactions and Customer activity to local Financial Intelligence Units. We have effective and reliable IT systems in place for monitoring and dedicated units to ensure data quality and ongoing support.

Implementation of Sanctions

We are committed to protection of human rights, countering financing of terrorism and proliferation of weapons of mass destruction. For this reason, in addition to fulfilling all statutory obligations related to sanctions imposed by United Nations, European Union and competent authorities of countries where we operate (Lithuania, Latvia, Estonia), we follow sanctions imposed by the Department of Treasury's Office of Foreign Asset Control (OFAC) of the United States of America, United Kingdom (HMT), Sweden and Norway. We screen all our Customers and their transactions against sanctions lists in real-time. We update our screening systems daily to reflect any updates or additions to the sanctions lists. We are precautious and reject any request to execute transaction, provide financial services or make a deal if it can violate sanctions restrictions imposed by above stated Sanctions Authorities. We report sanctions breaches and possible violations to the regulatory authorities.

Training and awareness

We recognize that prevention and identification of money laundering, financing of terrorism and proliferation of weapons of mass destruction or sanctions risks involves continuous employee professional development, awareness raising and the ability to keep pace with the trends and emerging risks in the area. For that purpose, we have implemented a continuous training programme which defines responsible persons for provision of trainings within the first line of defence and second line of defence; content and the audience, regularity and an audit trail of trainings provided. We design and continuously update the training programme to educate employees to recognize activities that can be related to money laundering, financing of terrorism and proliferation of weapons of mass destruction or sanctions and train what actions must be taken.

Business integrity

We highly value ethical behavior and endeavor to prevent any breaches of external and internal legal acts. Our employees can raise their concerns about perceived malpractice or wrongdoing according to Raising Your Concern process. In addition to our external Raise Your Concern form our Customers may also use third party reporting tools and whistleblowing procedures, such as those provided by local Banking Associations or supervisory authorities. Read further on our Raise Your Concern page.

Luminor

ABOUT US

Luminor is the leading independent bank in the Baltics and the third-largest provider of financial services in our region. We serve the financial needs of individuals, families, and companies. Just like our home markets of Estonia, Latvia, and Lithuania we are young, dynamic, and forward looking. Further information about us can be found at www.luminor.ee.

Liivalaia 45
10145 Tallinn
Estonia
www.luminor.ee

Media and Investor Relations contacts

For Media:
Ivi Heldna
Ivi.heldna@luminorgroup.com
+372 5231 192

For Investors:
Nick Turnor
nick.turnor@luminorgroup.com
+372 5306 7820