

# KOMMUNINVEST I SVERIGE AB

## Policy for combating financial crime

### C4P



Adopted by the Board of Directors	Document manager	Document owner	Information classification
27 October 2023	Specially appointed executive	Board of Directors	Public
<b>External regulations</b>			
Money Laundering and Terrorist Financing (Prevention) Act (2017:630) FFFS 2017:11 (EU) 2015/849 (EU) 2019/348 EBA/GL/2021/02 EBA/GL/2021/05 EBA/GL/2022/15 Act on Certain International Sanctions (1996:95)			
<b>Previous versions</b>			
30 September 2022			
<b>Background, etc.</b>			
<p>Kommuninvest i Sverige AB (hereinafter the “Company”) shall have good governance and internal control. The Board of Directors is responsible for ensuring that the Company complies with laws and applicable national and European regulations which govern the Company's operations. The Company's governance documents consist of documents adopted by the Board of Directors, the CEO, or the respective managers. The Board adopts policies and certain Board of Directors’ instructions. If necessary, these governance documents can be broken down into instructions which are confirmed by the CEO. Thereafter, the instructions can be broken down into more detailed descriptions, which are confirmed by the respective managers. The Board of Directors shall adopt policies annually and ensure that they are complied with and regularly assessed in the operations. The Board is ultimately responsible for ensuring that the Company has appropriate and efficient operations and a well-developed system for risk management and regulatory compliance.</p> <p>This policy covers the Company's Board of Directors, management, all employees, consultants, cooperating partners, agents, and service providers involved in the Company's operations. The policy is applicable to all parts of the operations and also includes outsourced operations and areas.</p> <p>The CEO is responsible for implementing and monitoring compliance with this policy. It is also the responsibility of the CEO to assess and update the content of this policy annually or when necessary and to present it to the Board of Directors, with any proposals for amendments.</p>			

## **1 Introduction**

Money laundering and terrorist financing, fraud, tax offences, and corruption are collectively referred to as financial crime.

The work to combat financial crime also includes obligations under agreed international sanctions, including regulations regarding violation of such sanctions.

In this policy, the Board of Directors of Kommuninvest i Sverige AB (the Company) has established internal rules to prevent and combat financial crime.

The Company will monitor and comply with decisions regarding international sanctions according to decisions by the EU and the Act on Certain International Sanctions.

The purpose of this policy is to ensure that the Company has the organisation, methods, and procedures to prevent financial crime.

## **2 Forms of work**

### ***2.1 Money laundering and terrorist financing***

The work to prevent money laundering and terrorist financing is based on a risk-based approach, where the measures are adapted in light of the risk of the operations being used for money laundering or terrorist financing. A general risk assessment in which the risk of the Company being used for money laundering and terrorist financing must be carried out and documented by the Company.

In connection with the general risk assessment, relevant risk factors such as which products and services are provided, which customers and distribution channels exist, and which geographic risk factors exist must be identified and analysed. Consideration must also be given to information that comes to light in connection with the Company's reporting of suspicious activities and transactions, as well as to information regarding money laundering and terrorist financing practices and other relevant information provided by authorities.

The scope of the general risk assessment will be determined taking into account the size and nature of the business and the risks of money laundering or terrorist financing that can be assumed to exist.

All of the Company's customers must be classified based on the risk of their use of the Company's products and services for money laundering and terrorist financing. The scope of measures to prevent such crime will depend on the risk classification of the customer. The risk classification is to be based on the risks identified in the general risk assessment and the Company's knowledge of the customer.

The Company must proceed from a good knowledge of the customer and an understanding of the customer's business, as well as the purpose and nature of the business relationship. Customer due diligence must be achieved and maintained for the duration of the customer relationship.

The Company will use reliable standards and methods to combat financial crime and prevent products, services, and distribution channels from being used by customers or staff for the purpose of financial crime.

## ***2.2 International sanctions***

Efforts to prevent the Company from contributing to a breach of rules and regulations regarding financial sanctions shall be carried out by obtaining the knowledge required to determine whether customers, counterparties, or others with whom the Company has business relations are subject to sanctions.

## ***2.3 Fraud***

The work to prevent customers from being exposed to fraud will be carried out with a risk-based approach, starting with an analysis of threats and vulnerabilities linked to the Company's products and services, but also taking into account other risks of fraud. Efforts to prevent the Company from being subjected to fraud by third parties will be based on the same principles.

## ***2.4 Corruption and bribery***

The Company does not accept corruption and bribery. The Company complies with Swedish legislation and other Swedish regulations in its operations and business relationships and, where applicable, with the legislation and regulations of other countries. The Company shall comply with the Anti-Corruption Institute's "Code to Prevent Corruption in Business". The Company will act such that the impermissible limits are avoided by a wide margin. Assessments are carried out, as necessary, together with an immediate superior and the Head of Legal and Procurement.

## ***2.5 Internal procedures against financial crime***

The work to prevent employees or other service providers from exposing customers or the Company to financial crime is carried out through, among other things, training initiatives, internal control, suitability assessment in connection with hiring and continuously during the employment relationship, duality in important decision-making processes, and other appropriate measures. The Company shall ensure that employees or other service providers have the possibility to report irregularities (see rules on whistleblowing in the Code of Conduct).

# **3 Organisation**

The Company applies the three lines of governance, risk management, and control.

### **3.1 Specially Appointed Executive (SAE) - first line of defence**

The specially appointed executive shall:

- be appointed by the CEO in accordance with the applicable rules and regulations;
- report to the Board of Directors and CEO in accordance with internal information and reporting procedures;
- be responsible for conducting an overall financial crime risk assessment and, annually or as necessary, reviewing and updating the risk assessment, policy, and instruction;
- ensure that the Company has internal procedures and guidelines and that these are regularly updated;
- verify and follow up that the measures, procedure, or other procedures decided by the Company are implemented in its operations.

The specially appointed executive may appoint one or more persons to assist them and delegate authority to them. If ambiguities arise regarding the handling of questions related to financial crime, the specially appointed executive is responsible for taking decisions on appropriate measures.

The specially appointed executive is the Head of Legal and Procurement.

### **3.2 Appointed Officer for Controlling and Reporting Obligations - second line**

The appointed officer for controlling and reporting obligations shall:

- be appointed by the CEO in accordance with the applicable rules and regulations;
- report to the Board of Directors and CEO in accordance with internal information and reporting procedures;
- regularly report on any risk analysis carried out and on risks and deficiencies, as well as on proposals for action. Reporting will be done in accordance with the internal information and reporting procedures;
- verify that the Company can maintain regulatory compliance in respect of financial crime prevention measures;
- verify that the Company implements and applies external and internal rules;
- verify how the Company identifies, assesses, and manages the risk of being exploited for financial crime;
- provide advice and support to employees regarding financial crime, as well as information and training;

- ensure that information is provided to relevant authorities in cases of suspected financial crime;
- be responsible for continuously monitoring information on new trends and patterns used, methods that can be used in financial crime, regulatory changes, and other information from organisations, authorities, and other bodies in the field.

The appointed officer for controlling and reporting obligations may appoint one or more persons to assist them and delegate authority to them. It is a requirement that this person is independent from the functions in the first line of defence which are to be monitored and verified.

The appointed officer for controlling and reporting obligations is the Chief Compliance Officer.

### **3.3 Internal audit - third line**

The Company has an internal audit function that reports to the Board of Directors. Internal audit works pursuant to guidelines established by the Board of Directors and the Company (the Board of Director's instruction for control functions).

## **4 Control measures, etc.**

The Company will implement control measures to mitigate the risks of financial crime. Control measures can take a variety of forms, such as restrictions on the product or service, customer due diligence measures, auditing measures, training of staff, etc. The control measures that are implemented are to mitigate the identified inherent risk.

Once a risk has been identified that needs to be mitigated, the mitigating measures will be taken into consideration and implemented in relation to both new and existing customers, as well as new and existing products and services.

The compliance department will provide advice and support regarding ways to structure the mitigation measures. The business is responsible for deciding, based on the recommendations of the compliance department, on how the mitigation measures are to be structured.

Control measures include, *inter alia*:

- customer due diligence;
- checks against sanctions lists;
- customer risk classification;
- transaction review;
- preservation of relevant documents and data.

The CEO, together with the specially appointed executive, is responsible for ensuring that procedures and processes for risk analysis and control measures, as well as other procedures for financial crime prevention measures are implemented in accordance with applicable external and internal regulations.

## **5 Protection of employees, service providers, or others**

The Company shall ensure that there are procedures and measures in place to protect employees, service providers, or others who administer or report suspected financial crime. The Company shall also ensure that employees do not suffer retaliation for reporting financial crime.

Rules regarding reporting (whistleblowing) are set out in the Company's code of conduct.

## **6 Retention of data**

The Company applies the Data Protection Framework to its activities when processing personal data. Sensitive data may only be processed if it is necessary to carry out certain basic or enhanced customer due diligence measures. Data used in the auditing obligation and provided to the Financial Intelligence Unit takes precedence over the above-stated law and may not be disclosed to the data subject.

## **7 Training and suitability assessment**

The Company will conduct an ongoing training program that includes financial crime prevention measures. All staff members who deal with matters or have customer contacts where financial crime provisions may be applicable will receive training in this area.

The Company will have a procedure for assessing the suitability of employees who handle matters or have customer contacts where the provisions on financial crime may be applicable.

## **8. Monitoring and reporting**

The Company will monitor customer relationships on an ongoing and risk-based basis, in particular with regard to the use of the Company's products and services.

The appointed officer for controlling and reporting obligations shall ensure that information regarding financial crime or regarding property that may otherwise derive from criminal activity is promptly provided to the relevant authority. The specially appointed executive has operational responsibility for providing information to authorities.