

# **Anti-Fraud Policy of KELER Group**

## **Extract**

## I. INTRODUCTORY PROVISIONS

KELER Ltd. (hereinafter referred to as “KELER”) and KELER CCP Ltd. (hereinafter referred to as “KELER CCP”) (with KELER and KELER CCP jointly referred to as “KELER Group”) ensures the prevention, detection and investigation of any fraud at KELER Group in harmony with the provisions of the law, the guidelines of international and European financial supervisory authorities and recommendation No. 12/2022 (VIII.11) of the National Bank of Hungary on the establishment and operation of internal lines of defence and the management and control functions of financial institutions (hereinafter referred to as the “MNB Recommendation”). They implement the necessary measures to carry out the resulting tasks, identify the risks of possible fraud and provide for the introduction of the necessary mitigating measures. The purpose of the Anti-Fraud Policy (hereinafter: the “Policy”) is to summarise the principles of and determine the main guidelines for the anti-fraud activity of KELER Group based on the expectations and guidelines formulated by the management of KELER and the KELER CCP, taking into account the valid and effective legislation, regulatory guidelines and internal rules, which together define, promote and support the proper, legal, safe and prudent operation of KELER Group.

The Policy sets out the rules and guidelines for the handling of suspected, attempted and actual fraud in relation to the services provided by KELER Group, the procedures for recording and analysing information and data collected in the course of fraud management and the way in which the findings made based on the foregoing can be fed back into the business processes.

The purpose of the Policy is to determine the organisational environment, the function and the principles guiding the operation of the fraud prevention activity, which are designed to prevent and detect fraud in a proactive manner, minimising the potential financial losses incurred, and to prevent and minimise legal, supervisory and reputational damage to KELER Group.

The senior management of KELER and KELER CCP is committed to ensuring that KELER Group conducts its business activities according to the strictest standards of integrity in order to maintain the confidence of its clients, business partners and employees.

## II GENERAL PROVISIONS

### 1. Scope of the Policy

The fraud prevention policy applies to the company as a whole, including all of its organisational units and activities. Natural persons and legal entities carrying out outsourced activities and expert or consultancy assignments are also subject to the anti-fraud requirements and standards.

### 2 Principles

In respect of the objectives and measures set out in the Policy, the following principles shall apply:

- a) **The protection of the Clients and KELER Group:** KELER Group is committed to preventing, detecting and effectively managing fraud in order to protect the money, investments, assets and property entrusted to it by its clients under all circumstances.
- b) **Fraud prevention:** in its anti-fraud activities, KELER Group focuses on prevention, aiming to minimise the risk of fraud, given that the recovery and collection of fraudulently obtained assets can be costly, of uncertain success and time-consuming and that fraud may result in serious reputational risks and loss of client confidence.
- c) **Proportionality:** in order to achieve the objectives of the fight against fraud, it is necessary to choose the means that are reasonable and best serve the achievement of the objectives, but do not cause undue burden or damage to either KELLER Group or its clients or partners.

- d) **Cooperation:** KELER Group and its clients and partners need to act together to combat fraud effectively, and KELER Group will use all means at its disposal to raise the awareness of its employees, clients and partners regarding fraud. At the same time, effective cooperation with law enforcement agencies, other authorities, domestic financial institutions, supervisory bodies, international repositories of value, the working groups of the Hungarian Banking Association and other specialist areas within the Group is to be achieved.
- e) **Zero tolerance:** there is zero tolerance shown for any intentional misconduct to the detriment of the clients or KELER Group, whether attempted or actual, and no distinction made between external and internal perpetrators of fraud.
- f) **Integrity and employee ethics:** employees involved in the fight against fraud must act in accordance with the rules governing the activities of their organisations, in accordance with the objectives, values and ethical standards defined.
- g) **Completeness, promptness, objectivity:** any suspected fraud shall be detected with the utmost completeness and the facts of the fraud shall be explored as soon as possible after its detection. This includes a factual determination of the circumstances of the fraud, the way of perpetration and the identity of the perpetrator where possible, as well as any deficiencies in the business processes and control systems that may have led to the suspected fraudulent events.
- h) **Feedback:** to prevent future occurrences of fraud that have taken place and to detect them in a timely manner, regular feedback is required to measure the effectiveness of the methodologies, screening automatisms and monitoring systems in place, so that timely action may be taken to address any deficiencies identified. In order to ensure objective and accurate backtesting, KELER Group maintains appropriate detailed records and the governing bodies and the areas concerned are regularly and comprehensively informed of any suspected cases of fraud, trends and actions taken during the period.
- i) **Innovation:** in order to detect fraud as early as possible, KELER Group strives to carry out monitoring activities, always adapted to the given external environmental impacts and trends, and to apply technological and technical procedures that enforce fraud prevention and protection against organised fraud, as well as process improvement measures and system improvements, where necessary.

### 3 Definition of key terms related to the anti-fraud activity

- a) **Fraud:** For the purposes of the Policy, fraud (including “csalás” as defined in the Criminal Code of Hungary) includes any intentional intellectual misuse and attempted misuse committed through deceptive conduct or actions for the purpose of obtaining illicit financial gain by using or circumventing the processes, tools or systems of KELER Group, to the detriment of a client of KELER Group or any other third party. Fraud may be committed by using, manipulating, or abusing the processes, tools or systems of KELER or KELER CCP intentionally, fraudulently and for the purpose of obtaining any illicit financial gain to the detriment of KELER or the KELER CCP and its clients, partners or third parties. Furthermore, any misuse of the systems and processes of KELER Group in a manner that causes damage to KELER Group shall be considered fraudulent. Damage shall include any loss of value of the assets of the injured party, any loss of financial benefits, as well as the costs necessary to compensate for the financial losses suffered by the injured party. Losses which cannot be quantified (e.g. loss of reputation) shall also be considered as damage. Corruption crimes against the integrity of public life (Chapter XXVII of the Criminal Code of Hungary) shall be considered a fraud even if KELER incurs no financial loss in connection therewith.

- b) **Fraud-related incident:** an internal or external fraud-related event that may result in a potential loss or an opportunity to violate a fraud prevention principle. An event that does not in itself result in a loss or exposure, but opens up the possibility for someone to commit a fraud shall also be regarded as a fraud-related incident. This includes the unauthorised disclosure of information qualifying as banking, securities or trade secret to an unauthorised third party for the purpose of obtaining an unlawful benefit.
- c) **Fraud risk:** the unanticipated financial, material or reputational risk arising from fraudulent activities of persons within or outside the organisation.
- d) **Fraud prevention activity:** A set of tools, methods and programmes designed to identify, analyse and mitigate fraud risk factors at the earliest possible stage within a financial organisation.
- e) **Client:** in the context of the fraud prevention activity, the term “client” shall be understood to include not only the clients affected by the services provided by KELER Group, but also suppliers and partners selling services to KELER Group, who are also subject to by the fraud prevention activity.
- f) **Fraud manager:** an activity carried out by the Compliance area, which is performed by staff members dealing with fraud prevention and fraud management.
- g) **Internal fraud:** Internal fraud shall be defined as losses resulting from intentional activities of fraud, misappropriation of assets, circumvention of laws or company rules with the involvement of at least one internal party, not including losses resulting from discrimination or social or cultural differences. Internal fraud includes internal fraud/theft/embezzlement/misappropriation or concealment of company resources, false accounting, misuse of information (breach of business or security secrecy, falsification of documents, unauthorised modification of transaction parameters).
- h) **External fraud:** intentional actions committed by a third party to commit a fraud, misappropriate assets or circumvent the law which do or may result in a loss to KELER Group or any of its clients. External fraud includes frauds perpetrated in connection with client transactions or orders, phishing type frauds, the misuse of the name of KELER or KELER CCP, social engineering type frauds, as well as frauds committed by using malicious IT programs.
- i) **Fraud committed by misrepresentation towards clients:** Suspected fraudulent transactions involving cleared payment transactions where a financial or securities transaction initiated by the client or a person who has obtained the client's data unlawfully is performed by means of a misrepresentation towards the account holder client, and the credit institution or CSD involved in the transaction or the Hungarian authority initiates the reversal or blocking of the funds with reference to the suspected fraud.
- j) **Human security risk:** information or circumstances that may allow a person, through the levels of authorization associated with a particular function or job, to get access to information or to banking, securities or business secrets or to make decisions on behalf of KELER Group which may be used or appropriated for profit or gain or which may cause damage to KELER Group.

### 3. Cooperation with other internal control functions and specialist areas:

Following the MNB Recommendation, KELER Group shall develop functions that take into account the specificity, scope and complexity of the service activities provided to its clients. In such scope, cooperation with other internal control functions and specialist areas (internal audit, risk management, security management, physical security, etc.) will be implemented. The Policy is a Group-wide regulatory document, which provides guidance and should be followed by KELER Group.

#### **4. The place of the fraud prevention function in the system of internal lines of defence:**

In line with the guidelines of the European financial supervisory authorities and the recommendations of international financial regulatory bodies, the MNB Recommendation has laid down the principles of internal regulation related to the prevention and management of fraud, which KELER Group incorporates into and adheres to in its activities.

The Policy covers the entire organisation (including governing bodies and the organisational units performing internal control functions) and all activities and services of KELER Group. The preventive activity is embodied on the first level in the fraud mitigation control processes and related audits embedded in the business processes. As part of the preventive activity, there are control points incorporated into the business processes - as well as warning signals and thresholds in the systems serving the business processes - to allow the timely detection and, where possible, the prevention of any fraud or attempted fraud and to minimise the damage caused. The required internal lines of defence against fraud shall be implemented at group level.