POLICY	
Title:	**ANTI FRAUD POLICY**
Process Group:	**ENTERPRISE RISK MANAGEMENT**
Process Owner:	**COMPLIANCE ROMANIA**
Effective Date:	**21/10/2024**
Summary:	The Policy describes the rules and main guidelines regarding the management of fraud incidents that may occur in Telekom Romania Mobile Communications S.A. companies and sets the necessary measures and control mechanisms to prevent such incidents.

	POSITION	**SIGNATURE**
Created by:	Alina Elena Dogaru Compliance Specialist	
Reviewed by:	Iulia Andreea Banciu Head of Legal, Data Privacy, Compliance, Environment & ISO Lead	
Approved by:	Approved by the Telekom Romania Mobile BoD in the meeting number 307 held on 21/10/2024	

This Policy has been acknowledged by the Executive Director Internal Audit OTE Group.

DOCUMENT HISTORY LOG		
Version	**Date**	**Description of Changes**
1.0	11/10/2016	Document adopted and transposed in Telekom template after approval by BoD. Code update from PL.ERM.07 (previously Cosmote Fraud Policy) to PL01.ERM.03 (integrated). Entered into force 11.10.2016
2.1	16/02/2018	Alignment to OTE Group Policy version 2.1 Update of scope to include provisions on anti-bribery and area of application to TKR and TKRM Updates according to current Organizational Chart
3.0	15/01/2024	Update after segregation
4.0	21/10/2024	Adopt and approve the new Anti- Fraud Policy in Telekom Romania Mobile, replacing the existing Anti – Fraud Policy as in force since 16.02.2018

Table of Contents

1) Preamble

In modern times financial crime is evolving rapidly and constitutes a major problem for companies worldwide. All companies, irrespective of their size or activity, are vulnerable to fraud. Furthermore, the ever-growing use of technology and the internet, in combination with the inadequacy or lack of effective control mechanisms, has contributed to the rapid increase of fraud incidents in the corporate environment. Fraud incidents emerging within the companies cause significant financial losses, expose the company to regulatory or legal risks, affect its reputation, distort good governance and undermine its stakeholders' trust (e.g. customers, suppliers, employees, shareholders, society).

The offense of fraud is among the so-called "white-collar" crimes. Usually, the offenders come from within the company and are employees or/and executives committing financial crimes or other illegal business activities in the context of their professional activities. It is typical that "white-collar" crimes are not usually included in the circle of traditional crimes and stereotypical criminality, however the losses caused are often particularly important.

At Telekom Mobile, "white-collar" crimes and other similar offenses are not tolerated.

The adoption of preventive measures following the identification and assessment of relevant risks and the consistent action against "white-collar" crimes constitute, thus, persisting challenges and important components of a responsible corporate policy.

2) Purpose

The Anti-Fraud Policy (hereinafter "Policy") has been adopted in order to describe indicatively the most common types of fraud that may occur in the corporate environment and may harm the interests of Telekom Mobile, to record the control mechanisms and safeguards adopted for the prevention and detection of fraud and to inform employees and third parties regarding the internal reporting channels adopted by the Company in order to submit reports on fraud incidents that have come to their attention.

In particular, this Policy aims to create a framework ensuring:

- the effectiveness of measures and control mechanisms adopted with respect to the prevention and detection of fraud incidents,
- the description of the main principles and rules adopted by Telekom Mobile to deal with fraud incidents, as well as the actions on behalf of Telekom Mobile employees at all levels to defend themselves against risks arising from fraud incidents,
- the existence and maintenance of a healthy work environment, where employees feel safe to report fraud incidents without fear of retaliation,
- the promotion of dialogue and awareness on fraud issues via training programs and awareness campaigns,
- the achievement of high-level business integrity through proper and effective corporate governance and internal control and transparency mechanisms to tackle fraud incidents.

Fighting fraud and bribery is part of the Compliance Management System (CMS) and of OTE Group corporate culture. The Compliance Management System has been certified according to ISO 37001:2016 (Anti-bribery management systems).

3) Scope - Definitions

3.1 The Policy applies to Telekom Mobile by a decision of its competent body.

3.2 The Policy applies for the investigation of all fraud cases committed by Telekom Mobile employees, irrespective of the status/position/title of persons involved, which cause or could cause financial loss or/and harm Telekom Mobile reputation.

3.3 For the purposes of this Policy, the following definitions apply:

- **OTE Group:** The parent company OTE S.A. and the affiliated companies of OTE S.A., within the meaning of article 32 of Law 4308/2014.
- **Company:** Telekom Mobile.
  - **Employees:** Every person working at the Company, irrespective of the nature of their activities, the type and duration of their employment, irrespective of whether their employment is full or part-time, permanent or seasonal, from the company's premises or remotely. In particular:
  - persons working at the Company under an employment contract or seconded employees or in-house lawyers,
  - persons working at the Company as independent contractors or providers of independent services or under any other type of contract,
  - persons employed by third companies under project contracts assigned to them by a Group company,
  - any person working under the supervision and direction of contractors, sub-contractors and suppliers,
  - persons belonging to the administrative or management body of the company.

4) Type of access

The Policy is posted on the corporate intranet and access to it is permitted to all employees of the company. The distribution of this document outside the company is not allowed.

5) Definition – Types of fraud

In the context and for the purposes of this Policy, **fraud** means any action, omission or tolerance on behalf of any employee, who knowingly presents false facts as true or fraudulently conceals or withholds true facts, aiming to cause damage or financial loss to foreign property or to obtain illegal pecuniary advantage for his own or other's benefit.

According to the Association of Certified Fraud Examiners (ACFE), **corporate fraud** is a broad concept that may take the following forms, briefly described below in Figure 1[1]:

- Embezzlement / theft, including misappropriation or removal of company's assets.
- Falsified / False reports, usually in the form of falsification of financial statements, accounting records or other company files, in order to obtain personal or business benefit. This concerns indicatively falsified or false/forged documents, such as certificates, attestations, fabricated invoices, etc.
- Active & Passive Bribery
- Conflicts of Interest

[1] *National Transparency Authority: Guide for Managing Corruption & Fraud Risks (Version 1.0, February 2021)*

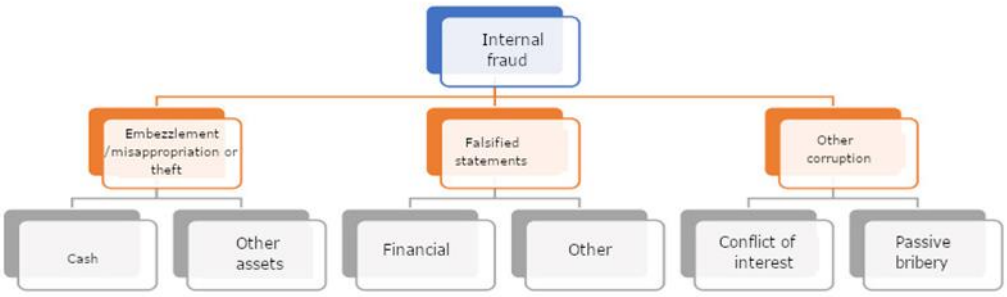

Figure 1: Types of internal fraud / corruption

The most common **types of internal fraud** with some indicative examples/scenarios that may occur in the corporate environment are the following:

- **Theft, embezzlement, fraud, computer fraud :** Money and assets belonging to the company, to which the offender has access due to their position or status and removes or misappropriates them, or offender who uses fraudulent means in order to damage foreign property and obtain illegal benefit.

  Examples: theft of corporate property (e.g. objects, equipment, materials, machinery, etc.), embezzlement of cash & coupons, fabricated invoices for products not delivered or for services not rendered to the company, overcharging for corporate travel expenses, personal expenses recorded as business expenses, use of the company assets for personal benefit, etc.

- **Active & Passive Bribery regarding public sector employees & political persons:** Offer or acceptance of a benefit for an action or omission within the scope of or contrary to the employee's duties.

  Examples: giving bribes to civil servants for processing corporate affairs, undertaking of public procurement due to sponsorships to political persons, donations to political parties to gain unfair advantage, etc.

- **Active & Passive Bribery in the private sector:** Especially for those working or providing services in any capacity or relationship in the private sector and, in the exercise of their business activity, request or receive, directly or indirectly, any unfair benefit of any nature in return for action or omission in breach of their duties.
- Examples: a gift from a candidate supplier to a company's employee in order to be selected in a tender, a gift to a manager in order to receive a positive evaluation, etc.

- **Forgery and falsification of accounting data, files, financial statements:**

  Examples: Falsified or false/forged documents/records/files (physical or electronic) in order to obtain personal or business benefit. Publication of improved financial results compared to the actual condition of the company aiming, for example, to attract investors or achieve concessional borrowing, etc. Or on the contrary, publication of financial results depicting company in an adverse financial position compared to the actual one, aiming for example to receive government grants, funds, aid, etc.

- **Insurance fraud:** False statements (e.g. the beneficiary provides false information to reduce the insurance cost or receive a higher insurance compensation), "setting up" fake accidents to receive compensations, identity theft, forged insurance contracts, etc.

- **Intellectual property fraud:** Fraud concerning patents, copyright, design rights, etc.

  Examples: the 'quid pro quo' disclosure to competitors of trade secrets, studies & know-how, the use of tools/material/data of the company for personal use and benefit, etc.

- **Cyber fraud:** This category includes incidents where technology and internet are used to commit fraud.

  Examples: hacking, ID fraud, credit card fraud, malware, ransomware, social engineering, clone websites etc.

- **Insider trading:** Access to sensitive business information that may be available to someone due to their job or position (e.g. executive, member of the BoD, etc.) and may be used for the benefit of themselves or a close person.

  Examples: information on a future investment or event that may affect share price or products price (e.g. merger, acquisition, sale, purchase, etc.), disclosure of commercial strategy etc.

- **Procurement fraud:** This category includes cases of bypassing the rules described in Procurement Policy and relevant corporate procedures.

  Examples: invoices for goods/services without matching to an existing purchase order, "splitting" of orders to bypass approval limits, tailor-made tenders, direct awards under non-transparent terms, contracts concluded by unauthorized executives/units, etc.

- **Ponzi scheme fraud[2]:** Fraud based on an investment "pyramid". The investment pyramid is an illegal investment scheme consisting of paying returns to older investors from the money paid in by new investors, instead of the net profits that should accrue from real investments.

- **Conflict of Interests:** Any situation in which the ability of independent evaluation, judgment or decision of an employee of the company is affected or may be affected by personal interest.

  Examples: a conflict of interests may arise from a competitive secondary occupation of an employee or when for example a company's executive is at the same time board member of a major supplier of the company or when a close relative of a company's manager undertakes by direct award an important project of the company, etc.

- **Breaches of anti-trust law:** Agreements or/and concerted practices with competitors, suppliers, etc., which have as their object or effect the prevention, restriction or distortion of competition as well as unilateral improper conduct (e.g. abuse of dominant market position).

  Examples: agreements with competitors to exchange information that harms competition, fixing purchase & sale prices and transaction terms & conditions, restriction of production, allocation of markets, boycotts, exclusivity clauses, tying and bundling, etc.

- **Money laundering:** A process by which the offenders conceal the illegal origin of their assets by covering up or eliminating the traces of the criminal acts from which the illegal proceeds were derived. They typically use underground financial systems to carry out transactions and payments beyond the surveillance mechanisms in order to introduce illicit money into the official economy and use it after laundering it.

  Examples: money laundering may occur for example through the establishment and operation of virtual companies, real estate investments, establishment and operation of offshore companies, use of cryptocurrencies, etc.

6) Fraud Prevention Measures

The Management of the company is responsible to take measures aiming to prevent and detect fraud and other irregularities in the context of its business activity and internal operation.

[2] The term "Ponzi scheme" is attributed to Charles Ponzi (1882-1949), American investor and swindler who invented this scheme during the 1920s.

Depending on the duties and activities assigned, the company shall appoint the competent persons in order to handle issues related to preventing and combating fraud and shall appropriately inform its employees/partners to this regard.

The Management of the company must perform their duties by demonstrating due diligence with respect to the performance of their professional activities, a principle reflected at least by taking the following preventive measures.

6.1) Adopting a strategy to prevent, detect and combat fraud

The adoption of a corporate strategy in which the prevention and fight against fraud will be at the center of company's interest is vital for dealing with fraud phenomena. The Management of the company is committed to adopt (tone at the top) an integrated program aiming to effectively handle these incidents and therefore secure the company's financial interests, create an ethical and transparent working environment and foster a culture of integrity.

The abovementioned program, which is depicted in this Policy, covers all stages of the anti-fraud cycle, i.e. prevention, detection and response by adopting corrective and other measures.

6.2) Risk Analysis & Fraud Risk Assessment

An integral part of an effective anti-fraud program is the systematic identification, recording and assessment of fraud risks within Telekom Mobile (Fraud Risk Assessment).

The Fraud Risk Assessment is carried out by the competent business units, and is integrated in the one carried out by the competent bodies of OTE Group, namely the ones under the Head of Business Security and Continuity OTE Group and the Executive Director Compliance, Enterprise Risk Management (ERM) & Insurance OTE Group, in order to identify risks related to fraud in specific areas of the company's operation (e.g. sales, procurement, accounting etc.).

This assessment, which shall be carried out at regular intervals or/and whenever deemed necessary, assesses the existing control mechanisms for fraud prevention and detection and sets any additional necessary measures for limiting or eliminating the identified fraud risks. During the Fraud Risk Assessment, past fraud cases shall be taken into account, inter alia.

The competent business units update the relevant fraud risks questionnaires, organize working groups, collect and assess the results, recommend measures and monitor the implementation of the respective measures.

6.3) Proper selection of employees and partners

The human factor is crucial for the success of a business. Recruiting the company's business units with capable and reliable personnel complying with the principles and values arising from the Telekom Mobile Code of Conduct and Policies is essential for the effective operation of the company and the avoidance of fraud incidents. Consequently, the company must ensure the proper selection of employees, assign tasks according to their duties and expertise and regularly monitor them.

The suitability of an employee to perform their duties shall be re-assessed through periodic evaluations in which the professional competence, reliability and integrity are evaluated. In addition, the employee shall annually declare that they have become aware and comply with the Policies of the Compliance Management System and that their interests (including the interests of their close family members) are not in conflict with Telekom Mobile interests. Special attention shall be paid upon filling vacancies in positions in which Fraud Risk Assessment has demonstrated that the exercise of the same job duties by an employee over time increases fraud risks. In these areas, the periodic change of the employee duties shall be considered as a possible tool to limit fraud risks.

The same principles of merit-based selection and transparency also govern the selection of Telekom Mobile partners, that are evaluated based on criteria and procedures included both in Procurement Policy and in relevant Telekom Mobile Processes. The company requires the supplier to comply with the principles included in the Supplier Code of Conduct, reflecting the ethical, social and

environmental commitments of the company and expects those principles to be adopted by its partners as well.

The risks arising from cooperation with third parties shall be assessed on a compliance perspective, therefore the business units submit a request for an integrity check and suppliers' evaluation according to compliance criteria, to the Compliance Department.

6.4) Segregation of duties - Clear information and transparency

The company's competent business units must allocate and clearly separate the employees' responsibilities (segregation of duties) so as to ensure that there will be separate tasks performed in a transparent way and that no employee will have the end-to-end control and responsibility of a project or process, which could potentially result in conflicts of interest situations and fraud incidents. Moreover, for the same reasons, the assignment of duties and the supervision of employees shall be conducted pursuant to the "4-eyes principle".

The company must also have corporate policies/procedures for all its operations and activities, which must be adopted and communicated in a clear and comprehensive way and shall provide to personnel clear guidelines and instructions, through its management, in order to perform their duties.

In addition, the company must ensure the establishment of clear rules of representation, signature, approvals and access and promote transparency in business decision-making.

When conducting transactions, written and detailed documentation is required to accompany the transactions and present a full and accurate description of the individual stages up to the completion of the transaction. Important transactions must be documented, as required by the law or/and company policies /procedures and the documentation shall be archived in an appropriate form.

6.5) Implementation of control mechanisms

The adoption of control mechanisms and the automation through information systems guarantee that the company's operations and systems function properly and safely in order to prevent fraud and cyber-attack incidents and that any weaknesses and vulnerabilities are immediately detected. Indicatively, the company adopts the following control mechanisms:

- Physical access controls (e.g. security personnel, alarm, monitoring & video surveillance systems, access cards, etc.).
- Logical access controls (e.g. passwords, user authentication, 2-factor authentication, digital signatures, etc.).
- Antivirus, anti-spam, anti-spyware software, firewalls, etc.
- Encryption of data and communications
- Intrusion detection & prevention systems (IDS/IPS, penetration/security testing, vulnerability scans, code robustness analysis, etc.)

In areas where the Fraud Risk Assessment has revealed high fraud risk, strict control measures are required and their implementation shall be documented in writing in order to be verified.

6.6) Information-Training

Telekom Mobile focuses on providing suitable and continuous training and information to its employees, as one of the most effective methods to prevent and fight fraud.

All employees are informed, in induction trainings upon the beginning of their employment, on this Policy and on matters regarding fraud and sanctions imposed for committing fraud.

Furthermore, in the context of the Compliance Training Program, Telekom Mobile employees participate in training sessions (in person and digital), inter alia, with respect to anti-fraud, while

employees working in sensitive areas or units exposed to higher fraud risks receive, at regular intervals and if deemed necessary, in-depth training focusing on fraud issues related to their duties.

The members of the company's Board of Directors are also obliged to attend such training programs on fraud issues, during their term of office.

6.7) Internal and external audits

Conducting regular, periodic and special audits is an effective tool to prevent and detect fraud incidents within the company. These audits may be carried out either by the internal auditors (**internal audit**), or by external bodies, such as state auditing bodies and statutory auditors/accountants from audit firms (**external audit**).

Internal and external audits are necessary in order to evaluate and certify the accuracy and correctness of the company's financial statements and they also contribute to the prevention and disclosure of errors, mistakes, omissions as well as fraud incidents.

In particular, in order to monitor the proper implementation of the process regarding logical access requirements described above under 6.5, the relevant audits are carried out by the competent units under the Security & External Affairs Director.

7) Detection and Response to fraud incidents

7.1. Main principles

Telekom Mobile is looking to the integrity of their employees and acknowledge their important role in prevention, detection and disclosure of fraud incidents. Therefore, employees are encouraged to always be alert and report without delay any fraud incident that has come to their attention. Telekom Mobile encourages both employees and third parties (e.g. suppliers, partners, etc.) not to hesitate to report fraud incidents and embraces their important role in shaping a culture which favors the prevention, detection and response to such incidents.

Any misconduct or other irregularity detected or suspected, must be immediately disclosed through the internal reporting channels adopted by Telekom Mobile which are mentioned below in paragraph 7.2 of this Policy.

7.2. Internal Reporting Channels

The company has established internal reporting channels that can be used by employees or/and third parties in order to address their reports regarding suspicions or incidents of fraud. The following internal reporting channels are available:

- **E-mail**:
  whistleblowing.mobil.ROU02@telekom.ro
  raportare.nereguli.mobil.ROU02@telekom.ro

- **Postal address**
  Attn: Compliance Department, Expozitiei Boulevard no.1C, Expo building, 3rd floor, postal code: 012101, 1st District, Bucharest, Romania

Further information on the internal reporting channels are provided in **Whistleblowing & Non-Retaliation Policy.**

In addition, employees must immediately inform their direct supervisors once they become aware of fraud incidents while performing their duties.

7.3. Internal investigations

7.3.1) Responsibilities

The investigation of potential fraud cases falls under the exclusive competence of Compliance Department. The Head of Legal, Data Privacy, Compliance, Environment & ISO has the obligation to assign responsibilities regarding the carrying out of investigations of compliance related reports (including fraud incidents), monitor the implementation and completion of the abovementioned investigations (Case Management), appoint case managers at its discretion and is entitled to recommend to the respective competent business unit appropriate measures and sanctions in case of breaches (Consequence Management).

In order to fulfill this role, the Head of Legal, Data Privacy, Compliance, Environment & ISO may request, during investigations or other actions, the contribution of employees or/and partners or engage external consultants, when required.

The **OTE Audit Committee** examines the results of the investigation for particularly serious reports in relation to the breach of the policies and procedures of the Company and the Group Companies as well as of the legislation in force (including fraud incidents), by virtue of the provisions of the Compliance System in force.

7.3.2) Investigation process

The internal investigation is carried out to identify and handle fraud incidents within the company which have caused or may cause financial loss to the company or/and harm its reputation. Safeguarding company's legitimate interests as well as preventing and punishing fraud offenses within it is the basis of approaching internal investigations and enabling the company to conduct them. No investigation can be carried out at company level in a way replacing the competent state bodies or obstructing in any way the investigation by the competent police or judicial authorities. In case of doubt concerning the implementation, applicability and sanctions provided for by the legal framework in force, the Legal Department should be consulted.

The investigation includes the following stages:

1. Receipt of the report
2. Plausibility check of the report
3. Preparation of the investigation plan & appointment of case manager/investigator
4. Collection of evidence & interviews
5. Preparation of the Investigation Report

All the investigation stages, as well as its results shall be documented in writing.

Detailed information on the investigation process and the individual actions required is provided in the **Compliance Management Process-Case Management**.

7.3.3) Measures

Following the completion of the investigation and the submission of the Investigation Report to the competent management bodies, the appropriate measures in each case (e.g. disciplinary sanctions, termination of the employment contract, etc.) are decided.

The Legal Department assists the investigation team at all stages of investigation, providing legal advice and guidance and upon completion of the investigation it examines whether the conditions of the law are met in order to file a report to the Authorities, based on the conclusions of the Investigation Report. The Legal Department or, after consultation with it, the Executive Director Compliance, ERM & Insurance OTE Group or the company's Compliance Officer shall contact the Authorities regarding fraud incidents.

In particular with respect to cyber-attacks, malicious third-party attacks and other serious security incidents, which may cause significant financial loss or harm the company's reputation, such as:

- unauthorized access to company's information systems,
- unauthorized file export from company's information systems,
- alteration of data/files from company's information systems,
- unauthorized use of services or resources,
- distributed denial-of-service (DDoS) etc.

all necessary measures must be taken immediately to deal with the incident and limit the damage; for example, access must be immediately blocked, the accounts of users involved must be immediately deactivated and the competent Authorities must be informed, as provided for by the aplicable legislation.

8) Confidentiality and Personal Data Protection

Internal investigations regarding fraud incidents are carried out in confidentiality and secrecy by the Compliance Department. The processing of personal data when handling the reports and conducting investigations for fraud incidents is subject to the provisions of Regulation (EU) 2016/679 ("GDPR") and shall be carried out pursuant to the respective Telekom Mobile Policies.

The company is the data controller for the personal data processed and kept in relation to the submitted reports regarding fraud incidents. To this end, the company takes the appropriate technical and organizational measures to guarantee the confidential management of reports and the protection of data and to ensure that the personal data that are absolutely necessary and appropriate in the context of pursuance of the processing purposes to be collected, while data obviously irrelevant to the handling of the specific report or excessive, are not collected, or, if collected accidentally, shall be immediately deleted.

9) Protection of the reporting person

The whistleblower's identity is not disclosed to anyone beyond the authorized members of the personnel who are responsible to receive and follow-up on fraud reports, without the explicit consent of the whistleblower. Notwithstanding the above, the identity of the whistleblower and any other information related to the report may be disclosed, following prior communication with the Legal Department of the company, only where there is an obligation imposed by Union or national law. In this case, the whistleblower shall be informed in writing before their identity is disclosed.

Telekom Mobile takes all necessary measures to ensure that persons providing information on possible fraud incidents, believing reasonably and in good faith that these reports are plausible, will be protected.

Any form of retaliation against the persons reporting fraud incidents is prohibited, including threats of retaliation and attempts of retaliation.

Detailed information regarding the protection of the whistleblower's identity and the prohibition of retaliation against the whistleblowers is provided in **Whistleblowing and Non-Retaliation Policy**.

10) Consequences of the violation of this Policy

Any violation of this Policy may result in liability risks for Telekom Mobile or/and the members of their corporate bodies or/and their officers/employees and subsequently incur disciplinary or other sanctions against those violating the Policy. Moreover, any violation of this Policy may cause

adverse legal consequences (criminal or civil, such as the obligation for compensation) against Telekom Mobile, as well as against those violating the Policy.

11) Entry into force – Amendment

The Policy is amended when it is deemed necessary, taking into consideration the effectiveness of its implementation, the need to amend it as well as possible changes in the legal and regulatory framework.