POLICY	
Title:	**POLITICA ANTI-FRAUDA**
Process Group:	**MANAGEMENTUL RISCULUI INTREPRINDERII**
Process Owner:	**CONFORMITATE ROMANIA**
Effective Date:	**21/10/2024**
Summary:	Politica descrie regulile și principalele linii de conduită privind gestionarea incidentelor de fraudă care pot apărea în cadrul companiilor Telekom Romania Mobile Communications S.A. și stabilește măsurile și mecanismele de control necesare pentru a preveni astfel de incidente.

	POSITION	**SIGNATURE**
Created by:		
Reviewed by:		
Approved by:	Aprobat de Consiliul de Administratie Telekom Romania Mobile in sedinta numarul 307 din 21/10/2024	

Această Politică a fost recunoscută de Directorul Executiv de Audit Intern al Grupului OTE.

DOCUMENT HISTORY LOG		
Version	**Date**	**Description of Changes**
1.0	11/10/2016	Document adoptat și transpus în modelul Telekom după aprobarea de către Consiliul de Administrație. Actualizare cod de la PL.ERM.07 (anterior Politica de Fraudă Cosmote) la PL01.ERM.03 (integrat). A intrat în vigoare la 11.10.2016
2.1	16/02/2018	Aliniere la Politica Grupului OTE versiunea 2.1 Actualizarea scopului pentru a include prevederi privind anti-mita și zona de aplicare pentru TKR și TKRM Actualizări conform Organigramei actuale
3.0	15/01/2024	Actualizare dupa segregare
4.0	21/10/2024	Adoptarea și aprobarea noii Politici Anti- Fraudă în Telekom Romania Mobile, înlocuind Politica Anti-Fraudă existentă în vigoare din 16.02.2018

Table of Contents

1) Preambul

În epoca modernă, criminalitatea financiară evoluează rapid și constituie o problemă majoră pentru companiile din întreaga lume. Toate companiile, indiferent de dimensiunea sau activitatea lor, sunt vulnerabile la fraudă. Mai mult, utilizarea în continuă creștere a tehnologiei și a internetului, în combinație cu insuficiența sau lipsa unor mecanisme eficiente de control, a contribuit la creșterea rapidă a incidentelor de fraudă în mediul corporativ. Incidentele de fraudă care apar în cadrul companiilor provoacă pierderi financiare semnificative, expun compania la riscuri de reglementare sau juridice, îi afectează reputația, distorsionează buna guvernanță și subminează încrederea părților interesate (de exemplu, clienți, furnizori, angajați, acționari, societate).

Infracțiunea de fraudă se numără printre așa-numitele infracțiuni "gulerelor albe". De obicei, infractorii provin din interiorul companiei și sunt angajați și/sau directori care comit infracțiuni financiare sau alte activități de afaceri ilegale în contextul activităților lor profesionale. Este tipic faptul că infracțiunile "gulerelor albe" nu sunt de obicei incluse în cercul infracțiunilor tradiționale și al criminalității stereotipice, totuși pierderile cauzate sunt adesea deosebit de importante.

La Telekom Mobile, infracțiunile "gulerelor albe" și alte infracțiuni similare nu sunt tolerate .

Adoptarea măsurilor preventive în urma identificării și evaluării riscurilor relevante și acțiunea consecventă împotriva infracțiunilor "gulerelor albe" constituie, astfel, provocări persistente și componente importante ale unei politici corporative responsabile.

2) Scop

Politica Anti-Fraudă (denumită în continuare "Politica") a fost adoptată pentru a descrie orientativ cele mai comune tipuri de fraudă care pot apărea în mediul corporativ și pot dăuna intereselor Telekom Mobile, pentru a înregistra mecanismele de control și garanțiile adoptate pentru prevenirea și detectarea fraudei și pentru a informa angajații și terții cu privire la canalele interne de raportare adoptate de Companie pentru a prezenta rapoarte privind incidentele de fraudă care le-au fost aduse la cunoștință.

În special, această Politică își propune să creeze un cadru care să asigure:

- eficacitatea măsurilor și mecanismelor de control adoptate în ceea ce privește prevenirea și detectarea incidentelor de fraudă,
- descrierea principiilor și regulilor principale adoptate de Telekom Mobile pentru a face față incidentelor de fraudă, precum și acțiunile în numele angajaților Telekom Mobile la toate nivelurile pentru a se apăra împotriva riscurilor care decurg din incidentele de fraudă,
- existența și menținerea unui mediu de lucru sănătos, în care angajații se simt în siguranță să raporteze incidente de fraudă fără teamă de represalii,
- promovarea dialogului și conștientizării cu privire la problemele de fraudă prin intermediul programelor de instruire și a campaniilor de conștientizare,
- realizarea integrității de afaceri la nivel înalt prin guvernanță corporativă adecvată și eficientă și mecanisme de control intern și transparență pentru a combate incidentele de fraudă.

Combaterea fraudei și a mitei face parte din Sistemul de Management al Conformității (CMS) și din cultura corporativă a Grupului OTE. Sistemul de Management al Conformității a fost certificat conform ISO 37001:2016 (Sisteme de management anti-mită).

3) Domeniul de aplicare- Definitii

3.1 Politica se aplică Telekom Mobile printr-o decizie a organului său competent.

3.2 Politica se aplică pentru investigarea tuturor cazurilor de fraudă comise de angajații Telekom Mobile, indiferent de statutul/poziția/titlul persoanelor implicate, care cauzează sau ar putea cauza pierderi financiare și/sau dăunează reputației Telekom Mobile.

3.3 În sensul prezentei Politici, se aplică următoarele definiții:

- **Grupul OTE:** Compania mamă OTE S.A. și companiile afiliate ale OTE S.A., în sensul articolului 32 din Legea 4308/2014.
- **Compania:** Telekom Mobile.
- **Angajați:** Fiecare persoană care lucrează la Companie, indiferent de natura activităților sale, de tipul și durata angajării, indiferent dacă angajarea este cu normă întreagă sau cu timp parțial, permanentă sau sezonală, de la sediul companiei sau de la distanță. În special:
    - persoane care lucrează la Companie în baza unui contract de muncă sau angajați detașați sau avocați interni,
    - persoane care lucrează la Companie ca contractori independenți sau furnizori de servicii independente sau sub orice alt tip de contract,
    - persoane angajate de companii terțe în cadrul unor contracte de proiect atribuite acestora de către o companie din Grup,
    - orice persoană care lucrează sub supravegherea și direcția contractorilor, subcontractorilor și furnizorilor,
    - persoane aparținând organului administrativ sau de conducere al companiei.

4) Tip de acces

Politica este postată pe intranetul corporativ și accesul la aceasta este permis tuturor angajaților companiei. Distribuirea acestui document în afara companiei nu este permisă.

5) Definitie – Tipuri de frauda

În contextul și în scopurile acestei Politici, **frauda** înseamnă orice acțiune, omisiune sau toleranță din partea oricărui angajat, care prezintă în mod conștient fapte false ca fiind adevărate sau ascunde sau reține în mod fraudulos fapte adevărate, având ca scop provocarea de daune sau pierderi financiare proprietății străine sau obținerea unui avantaj pecuniar ilegal pentru beneficiul propriu sau al altora.

Conform Asociației Examinatorilor de Fraudă Certificați (ACFE), frauda corporativă este un concept larg care poate lua următoarele forme, descrise pe scurt mai jos în Figura 1[1]:

- Delapidare / furt, inclusiv însușirea ilegală sau îndepărtarea activelor companiei.
- Rapoarte falsificate / false, de obicei sub forma falsificării situațiilor financiare, a înregistrărilor contabile sau a altor fișiere ale companiei, pentru a obține beneficii personale sau de afaceri. Aceasta se referă la documente falsificate sau false/contrafăcute, cum ar fi certificate, atestări, facturi fabricate etc.
- Mită activă și pasivă
- Conflicte de interese

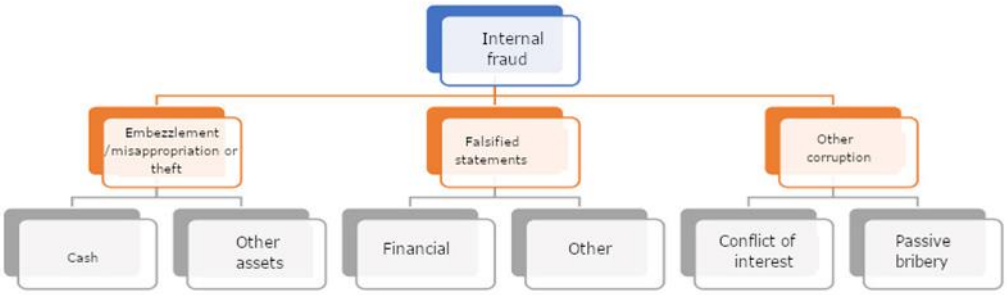

Figure 1: Types of internal fraud / corruption

Cele mai comune tipuri de fraudă internă cu câteva exemple/scenarii orientative care pot apărea în mediul corporativ sunt următoarele:

- **Furt, delapidare, fraudă, fraudă informatică:** Bani și active aparținând companiei, la care făptuitorul are acces datorită poziției sau statutului său și le îndepărtează sau și le însușește ilegal, sau făptuitorul care folosește mijloace frauduloase pentru a prejudicia proprietatea străină și a obține un beneficiu ilegal.

  Exemple: furtul proprietății corporative (de exemplu, obiecte, echipamente, materiale, mașini etc.), delapidarea de numerar și cupoane, facturi fabricate pentru produse nelivrate sau pentru servicii neprestate companiei, supraîncărcarea cheltuielilor de călătorie corporative, cheltuieli personale înregistrate ca cheltuieli de afaceri, utilizarea activelor companiei pentru beneficiu personal etc.

- **Mită activă și pasivă privind angajații din sectorul public și persoane politice:** Oferirea sau acceptarea unui beneficiu pentru o acțiune sau omisiune în limita sau contrar îndatoririlor angajatului.

  Exemple: oferirea de mită funcționarilor publici pentru procesarea afacerilor corporative, câștigarea achizițiilor publice datorită sponsorizărilor către persoane politice, donații către partide politice pentru a obține avantaje necinstite etc.

- **Mită activă și pasivă în sectorul privat:**

În special pentru cei care lucrează sau furnizează servicii în orice calitate sau relație în sectorul privat și, în exercitarea activității lor de afaceri, solicită sau primesc, direct sau indirect, orice beneficiu necinstit de orice natură în schimbul unei acțiuni sau omisiuni cu încălcarea îndatoririlor lor.

Exemple: un cadou din partea unui furnizor candidat către un angajat al companiei pentru a fi selectat într-o licitație, un cadou către un manager pentru a primi o evaluare pozitivă etc.

- **Falsificare și falsificarea datelor contabile, fișierelor, situațiilor financiare:**

Exemple: Documente/înregistrări/fișiere falsificate sau false/contrafăcute (fizice sau electronice) pentru a obține beneficii personale sau de afaceri. Publicarea unor rezultate financiare îmbunătățite în comparație cu starea reală a companiei având ca scop, de exemplu, atragerea investitorilor sau obținerea de împrumuturi concesionale etc. Sau, dimpotrivă, publicarea unor rezultate financiare care prezintă compania într-o poziție financiară nefavorabilă în comparație cu cea reală, având ca scop, de exemplu, primirea de subvenții guvernamentale, fonduri, ajutoare etc.

- **Fraudă de asigurare:** Declarații false (de exemplu, beneficiarul furnizează informații false pentru a reduce costul asigurării sau pentru a primi o compensație de asigurare mai mare), "organizarea" de accidente false pentru a primi compensații, furt de identitate, contracte de asigurare falsificate etc.

- **Fraudă de proprietate intelectuală:** Fraudă privind brevete, drepturi de autor, drepturi de design etc.
Exemple: dezvăluirea "quid pro quo" către concurenți a secretelor comerciale, a studiilor și a know-how-ului, utilizarea instrumentelor/materialelor/datelor companiei pentru uz personal și beneficiu etc.

- **Fraudă cibernetică:** Această categorie include incidente în care tehnologia și internetul sunt utilizate pentru a comite fraude.

Exemple: hacking, fraudă de identitate, fraudă cu carduri de credit, malware, ransomware, inginerie socială, site-uri web clone etc.

- **Tranzacții bazate pe informații privilegiate:** Accesul la informații sensibile de afaceri care pot fi disponibile cuiva datorită funcției sau poziției sale (de exemplu, executiv, membru al Consiliului de Administrație, etc.) și care pot fi utilizate în beneficiul propriu sau al unei persoane apropiate.

Exemple: informații despre o investiție viitoare sau un eveniment care poate afecta prețul acțiunilor sau prețul produselor (de exemplu, fuziune, achiziție, vânzare, cumpărare etc.), dezvăluirea strategiei comerciale etc.

- **Fraudă în achiziții:** Această categorie include cazuri de eludare a regulilor descrise în Politica de Achiziții și procedurile corporative relevante.

  Exemple: facturi pentru bunuri/servicii fără a corespunde unei comenzi de achiziție existente, "împărțirea" comenzilor pentru a eluda limitele de aprobare, licitații personalizate, atribuiri directe în condiții netransparente, contracte încheiate de către directori/unități neautorizate etc.

- **Fraudă de tip Ponzi** [1]**:** Fraudă bazată pe o "piramidă" de investiții. Piramida de investiții este o schemă ilegală de investiții care constă în plata de randamente investitorilor mai vechi din banii plătiți de investitorii noi, în loc de profiturile nete care ar trebui să provină din investiții reale.

- **Conflict de interese:** Orice situație în care capacitatea de evaluare independentă, judecată sau decizie a unui angajat al companiei este afectată sau poate fi afectată de interesul personal.

  Exemple: un conflict de interese poate apărea dintr-o ocupație secundară competitivă a unui angajat sau atunci când, de exemplu, un executiv al companiei este în același timp membru al consiliului de administrație al unui furnizor important al companiei sau când o rudă apropiată a unui manager al companiei preia prin atribuire directă un proiect important al companiei etc.

- **Încălcări ale legii antitrust:** Acorduri și/sau practici concertate cu concurenți, furnizori etc., care au ca obiect sau efect prevenirea, restricționarea sau denaturarea concurenței, precum și comportamentul unilateral necorespunzător (de exemplu, abuzul de poziție dominantă pe piață).

  Exemple: acorduri cu concurenții pentru a schimba informații care dăunează concurenței, fixarea prețurilor de cumpărare și vânzare și a termenilor și condițiilor de tranzacționare, restricționarea producției, alocarea pieței, boicoturi, clauze de exclusivitate, legarea și gruparea etc.

- **Spălare de bani:** Un proces prin care infractorii ascund originea ilegală a activelor lor prin acoperirea sau eliminarea urmelor actelor criminale din care au fost derivate produsele ilegale. Aceștia folosesc de obicei sisteme financiare subterane pentru a efectua tranzacții și plăți dincolo de mecanismele de supraveghere pentru a introduce bani iliciți în economia oficială și a-i utiliza după spălare.

  Exemple: spălarea de bani poate apărea, de exemplu, prin înființarea și funcționarea de companii virtuale, investiții imobiliare, înființarea și funcționarea de companii offshore, utilizarea criptomonedelor etc.

6) Masuri de prevenire a Fraudei

Conducerea companiei este responsabilă să ia măsuri care vizează prevenirea și detectarea fraudelor și a altor nereguli în contextul activității sale de afaceri și al funcționării interne.

În funcție de sarcinile și activitățile atribuite, compania va desemna persoanele competente pentru a gestiona probleme legate de prevenirea și combaterea fraudei și va informa în mod corespunzător angajații/partenerii săi în acest sens.

Conducerea companiei trebuie să își îndeplinească îndatoririle demonstrând diligența cuvenită în ceea ce privește desfășurarea activităților lor profesionale, un principiu reflectat cel puțin prin luarea următoarelor măsuri preventive.

6.1) Adoptarea unei strategii de prevenire, detectare si combatere a fraudei

Adoptarea unei strategii corporative în care prevenirea și lupta împotriva fraudei va fi în centrul interesului companiei este vitală pentru a face față fenomenelor de fraudă. Conducerea companiei se angajează să adopte (ton de la vârf) un program integrat care vizează gestionarea eficientă a acestor incidente și, prin urmare, să securizeze interesele financiare ale companiei, să creeze un mediu de lucru etic și transparent și să promoveze o cultură a integrității.

Programul menționat mai sus, care este descris în această Politică, acoperă toate etapele ciclului anti-fraudă, și anume prevenirea, detectarea și răspunsul prin adoptarea de măsuri corective și alte măsuri.

6.2) Analiza riscurilor si evaluarea riscului de frauda

O parte integrantă a unui program anti-fraudă eficient este identificarea, înregistrarea și evaluarea sistematică a riscurilor de fraudă în cadrul Telekom Mobile (Evaluarea Riscului de Fraudă).

Evaluarea Riscului de Fraudă este efectuată de unitățile de afaceri competente și este integrată în cea efectuată de organismele competente ale Grupului OTE, și anume cele subordonate Șefului Securității și Continuității Afacerilor din Grupul OTE și Directorului Executiv de Conformitate, Management al Riscului Întreprinderii (ERM) și Asigurări din Grupul OTE, pentru a identifica riscurile legate de fraudă în anumite domenii ale operațiunilor companiei (de exemplu, vânzări, achiziții, contabilitate etc.).

Această evaluare, care se va efectua la intervale regulate și/sau ori de câte ori se consideră necesar, evaluează mecanismele de control existente pentru prevenirea și detectarea fraudei și stabilește orice măsuri suplimentare necesare pentru limitarea sau eliminarea riscurilor de fraudă identificate. În timpul Evaluării Riscului de Fraudă, se vor lua în considerare, printre altele, cazurile de fraudă din trecut.

Unitățile de afaceri competente actualizează chestionarele relevante privind riscurile de fraudă, organizează grupuri de lucru, colectează și evaluează rezultatele, recomandă măsuri și monitorizează implementarea măsurilor respective

6.3) Selectia corespunzatoare a angajatilor si partenerilor

Factorul uman este crucial pentru succesul unei afaceri. Recrutarea unităților de afaceri ale companiei cu personal capabil și de încredere, care respectă principiile și valorile care decurg din Codul de Conduită și Politicile Telekom Mobile, este esențială pentru funcționarea eficientă a companiei și evitarea incidentelor de fraudă. În consecință, compania trebuie să asigure selectarea corespunzătoare a angajaților, să atribuie sarcini conform îndatoririlor și expertizei lor și să îi monitorizeze în mod regulat.

Adecvarea unui angajat pentru a-și îndeplini îndatoririle va fi reevaluată prin evaluări periodice în care sunt evaluate competența profesională, fiabilitatea și integritatea. În plus, angajatul va declara anual că a luat la cunoștință și respectă Politicile Sistemului de Management al Conformității și că interesele sale (inclusiv interesele membrilor apropiați ai familiei sale) nu sunt în conflict cu interesele Telekom Mobile. O atenție specială va fi acordată la ocuparea posturilor vacante în poziții în care Evaluarea Riscului de Fraudă a demonstrat că exercitarea acelorași sarcini de lucru de către un angajat în timp crește riscurile de fraudă. În aceste domenii, schimbarea periodică a îndatoririlor angajatului va fi considerată ca un posibil instrument pentru a limita riscurile de fraudă.

Aceleași principii de selecție bazată pe merit și transparență guvernează și selecția partenerilor Telekom Mobile, care sunt evaluați pe baza criteriilor și procedurilor incluse atât în Politica de Achiziții, cât și în Procesele relevante Telekom Mobile. Compania solicită furnizorului să respecte principiile incluse în Codul de Conduită al Furnizorului, reflectând angajamentele etice, sociale și de mediu ale companiei și se așteaptă ca aceste principii să fie adoptate și de partenerii săi.

Riscurile care decurg din cooperarea cu terții vor fi evaluate din perspectiva conformității, prin urmare unitățile de afaceri prezintă o cerere pentru o verificare a integrității și evaluarea furnizorilor conform criteriilor de conformitate, către Departamentul de Conformitate.

6.4) Segregarea sarcinilor- informare clara si transparenta

Unitățile de afaceri competente ale companiei trebuie să aloce și să separe clar responsabilitățile angajaților (separarea sarcinilor) astfel încât să se asigure că vor exista sarcini separate îndeplinite într-un mod transparent și că niciun angajat nu va avea controlul și responsabilitatea de la un capăt la altul asupra unui proiect sau proces, care ar putea duce potențial la situații de conflict de interese și incidente de fraudă. Mai mult, din aceleași motive, atribuirea sarcinilor și supravegherea angajaților se va efectua în conformitate cu "principiul celor 4 ochi".

Compania trebuie, de asemenea, să aibă politici/proceduri corporative pentru toate operațiunile și activitățile sale, care trebuie să fie adoptate și comunicate într-un mod clar și cuprinzător și să furnizeze personalului linii directoare și instrucțiuni clare, prin intermediul conducerii sale, pentru a-și îndeplini îndatoririle.

În plus, compania trebuie să asigure stabilirea unor reguli clare de reprezentare, semnătură, aprobări și acces și să promoveze transparența în luarea deciziilor de afaceri.

La efectuarea tranzacțiilor, este necesară o documentație scrisă și detaliată care să însoțească tranzacțiile și să prezinte o descriere completă și exactă a etapelor individuale până la finalizarea tranzacției. Tranzacțiile importante trebuie să fie documentate, așa cum prevede legea și/sau politicile/procedurile companiei, iar documentația va fi arhivată într-o formă adecvată.

6.5) Implementarea mecanismelor de control

Adoptarea mecanismelor de control și automatizarea prin sisteme informatice garantează că operațiunile și sistemele companiei funcționează corespunzător și în siguranță pentru a preveni incidentele de fraudă și atacurile cibernetice și că orice slăbiciuni și vulnerabilități sunt detectate imediat. În mod indicativ, compania adoptă următoarele mecanisme de control:

- Controale de acces fizic (de exemplu, personal de securitate, sisteme de alarmă, monitorizare și supraveghere video, carduri de acces etc.).

- Controale de acces logic (de exemplu, parole, autentificarea utilizatorilor, autentificare cu 2 factori, semnături digitale etc.).
- Software antivirus, anti-spam, anti-spyware, firewall-uri etc.
- Criptarea datelor și comunicațiilor

Sisteme de detectare și prevenire a intruziunilor (IDS/IPS, testare de penetrare/securitate, scanări de vulnerabilitate, analiză a robusteții codului etc.)

În domeniile în care evaluarea riscului de fraudă a evidențiat un risc ridicat de fraudă, sunt necesare măsuri stricte de control, iar punerea lor în aplicare trebuie să fie documentată în scris pentru a putea fi verificată.

6.6) Informare-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.

Telekom Mobile se concentrează pe furnizarea de instruire și informare adecvată și continua a angajaților săi, ca una dintre cele mai eficiente metode de prevenire și combatere a fraudei.

Toți angajații sunt informați, în cadrul instruirilor introductive la începutul angajării, cu privire la această politică și la aspecte legate de fraudă și sancțiuni impuse pentru comiterea de fraude.

În plus, în contextul Programului de training în materie de conformitate, angajații Telekom Mobile participă la sesiuni de instruire (în persoană și digitale), printre altele, în ceea ce privește antifrauda, în timp ce angajații care lucrează în zone sensibile sau unități expuse unor riscuri mai mari de fraudă primesc, la intervale regulate și dacă se consideră necesar, instruire aprofundată axată pe probleme de fraudă legate de atribuțiile lor.

Membrii Consiliului de Administratie al societatii sunt, de asemenea, obligati sa participe la astfel de traininguri pe probleme de frauda, pe durata mandatului lor.

6.7) Audituri interne si externe

Efectuarea de audituri regulate, periodice și speciale este un instrument eficient pentru prevenirea și detectarea incidentelor de fraudă în cadrul companiei. Aceste audituri pot fi efectuate fie de auditorii interni (**audit intern**), fie de organisme externe, cum ar fi organele de audit de stat și auditorii statutari/contabilii firmelor de audit (**audit extern**).

Auditurile interne și externe sunt necesare pentru a evalua și certifica acuratețea și corectitudinea situațiilor financiare ale companiei și contribuie, de asemenea, la prevenirea și dezvăluirea erorilor, greșelilor, omisiunilor, precum și a incidentelor de fraudă.

În special, pentru a monitoriza punerea în aplicare corespunzătoare a procesului privind cerințele de acces logic descrise mai sus la punctul 6.5, auditurile relevante sunt efectuate de unitățile competente din subordinea Directorului Securitate și Afaceri Externe.

7) Detectarea și răspunsul la incidentele de fraudă

7.1. Principii de bază

Telekom Mobile se uită la integritatea angajaților săi și recunoaște rolul lor important în prevenirea, detectarea și dezvăluirea incidentelor de fraudă. Prin urmare, angajații sunt încurajați să fie mereu atenți și să raporteze fără întârziere orice incident de fraudă care le-a ajuns la cunoștință. Telekom Mobile încurajează atât angajații, cât și terții (de exemplu, furnizori, parteneri etc.) să nu ezite să raporteze incidentele de fraudă și îmbrățișează rolul lor important în modelarea unei culturi care favorizează prevenirea, detectarea și răspunsul la astfel de incidente.

Orice abatere sau altă neregulă detectată sau suspectată trebuie să fie dezvăluită imediat prin canalele interne de raportare adoptate de Telekom Mobile, care sunt menționate mai jos în paragraful 7.2 al acestei Politici.

7.2. Canale interne de raportare

Compania a stabilit canale interne de raportare care pot fi utilizate de angajați și/sau terți pentru a răspunde raportărilor lor privind suspiciunile sau incidentele de fraudă. Sunt disponibile următoarele canale interne de raportare:

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

- **Adresa postala**

În atenția: Departamentul Compliance, Bulevardul Expozitiei nr.1C, clădirea Expo, etaj 3, cod poștal: 012101, Sector 1, București, România

Mai multe informații despre canalele interne de raportare sunt furnizate în **Politica privind avertizorii de integritate și nerepresaliile**.

În plus, angajații trebuie să-și informeze imediat superiorii direcți odată ce iau cunoștință de incidentele de fraudă în timp ce își îndeplinesc sarcinile.

7.3. Investigatii interne

7.3.1) Responsabilitati

Investigarea potențialelor cazuri de fraudă intră în competența exclusivă a Departamentului de Conformitate. Șeful departamentului juridic, confidențialitate a datelor, conformitate, mediu și ISO are obligația de a atribui responsabilități cu privire la efectuarea investigațiilor rapoartelor legate de conformitate (inclusiv incidente de fraudă), de a monitoriza implementarea și finalizarea investigațiilor menționate mai sus (Managementul de caz), de a numi manageri de caz la discreția sa și are dreptul de a recomanda unității de afaceri competente respective măsuri și sancțiuni adecvate în caz de încălcări (Consecință Management).

Pentru a îndeplini acest rol, șeful departamentului juridic, confidențialitate a datelor, conformitate, mediu și ISO poate solicita, în timpul investigațiilor sau altor acțiuni, contribuția angajaților și/sau a partenerilor sau poate angaja consultanți externi, atunci când este necesar.

Comitetul **de audit OTE** examinează rezultatele investigației pentru rapoarte deosebit de grave în legătură cu încălcarea politicilor și procedurilor Companiei și ale Companiilor din Grup, precum și a legislației în vigoare (inclusiv incidente de fraudă), în temeiul prevederilor Sistemului de Conformitate în vigoare.

7.3.2) Procesul de investigare

Investigația internă se desfășoară pentru a identifica și gestiona incidentele de fraudă din cadrul companiei care au cauzat sau pot cauza pierderi financiare companiei sau/sau pot afecta reputația acesteia. Protejarea intereselor legitime ale companiei, precum și prevenirea și pedepsirea infracțiunilor de fraudă din cadrul acesteia reprezintă baza abordării investigațiilor interne și a permiterii companiei să le desfășoare. Nicio anchetă nu poate fi efectuată la nivel de întreprindere care să înlocuiască organele competente ale statului sau să obstrucționeze în vreun fel ancheta de către autoritățile polițienești sau judiciare competente. În caz de îndoială cu privire la punerea în aplicare, aplicabilitatea și sancțiunile prevăzute de cadrul legal în vigoare, ar trebui consultat Departamentul juridic.

Ancheta include următoarele etape:

1. Primirea raportului
2. Verificarea plauzibilității raportului
3. Pregătirea planului de investigație și numirea managerului de caz/investigatorului
4. Colectarea de dovezi și interviuri
5. Pregătirea raportului de investigație

Toate etapele investigației, precum și rezultatele acesteia sunt documentate în scris.

Informații detaliate despre procesul de investigație și acțiunile individuale necesare sunt furnizate în **Procesul de management al conformității-Managementul cazurilor**.

7.3.3) Masuri

În urma finalizării investigației și a prezentării raportului de investigație organelor de conducere competente, se decid măsurile adecvate în fiecare caz (de exemplu, sancțiuni disciplinare, încetarea contractului de muncă etc.).

Departamentul juridic asistă echipa de investigație în toate etapele investigației, oferind consultanță și îndrumare juridică, iar la finalizarea investigației examinează dacă sunt îndeplinite condițiile legii pentru a depune un raport către autorități, în baza concluziilor Raportului de investigație. Departamentul juridic sau, după consultarea acestuia, Directorul Executiv Compliance, ERM & Insurance OTE Group sau Compliance Officer al companiei va contacta Autoritățile cu privire la incidentele de fraudă.

În special în ceea ce privește atacurile cibernetice, atacurile rău intenționate ale terților și alte incidente grave de securitate, care pot cauza pierderi financiare semnificative sau pot afecta reputația companiei, cum ar fi:

- accesul neautorizat la sistemele informatice ale companiei,
- exportul neautorizat de fișiere din sistemele informatice ale companiei,
- modificarea datelor/fișierelor din sistemele informatice ale companiei;
- utilizarea neautorizată a serviciilor sau resurselor,
- DDoS distribuit etc.

trebuie luate imediat toate măsurile necesare pentru a face față incidentului și a limita daunele; de exemplu, accesul trebuie blocat imediat, conturile utilizatorilor implicați trebuie dezactivate imediat și autoritățile competente trebuie informate, așa cum prevede legislația aplicabilă.

7) Confidentialitate si Protectia datelor cu caracter personal

Investigațiile interne privind incidentele de fraudă se desfășoară în confidențialitate și secret de către Departamentul de Conformitate. Prelucrarea datelor cu caracter personal la prelucrarea rapoartelor și efectuarea investigațiilor pentru incidente de fraudă este supusă prevederilor Regulamentului (UE) 2016/679 ("GDPR") și se va efectua în conformitate cu politicile Telekom Mobile respective.

Compania este operatorul de date pentru datele cu caracter personal prelucrate și păstrate în legătură cu rapoartele transmise privind incidentele de fraudă. În acest scop, compania ia măsurile tehnice și organizatorice adecvate pentru a garanta gestionarea confidențială a rapoartelor și protecția datelor și pentru a se asigura că datele cu caracter personal care sunt absolut necesare și adecvate în contextul urmăririi scopurilor de prelucrare care urmează să fie colectate, în timp ce datele în mod evident irelevante pentru gestionarea raportării specifice sau excesive, nu sunt colectate sau, dacă sunt colectate accidental, vor fi șterse imediat.

8) Protectia persoanei care efectueaza raportarea

Identitatea avertizorului nu este dezvăluită nimănui în afară de membrii autorizați ai personalului care sunt responsabili să primească și să urmărească rapoartele de fraudă, fără consimțământul explicit al avertizorului. Fără a aduce atingere celor de mai sus, identitatea avertizorului și orice alte informații legate de raportare pot fi divulgate, în urma unei comunicări prealabile cu departamentul juridic al societății, numai în cazul în care există o obligație impusă de dreptul Uniunii sau de dreptul intern. În acest caz, avertizorul este informat în scris înainte ca identitatea sa să fie dezvăluită.

Telekom Mobile ia toate măsurile necesare pentru a se asigura că persoanele care furnizează informații despre posibile incidente de fraudă, considerând în mod rezonabil și cu bună credință că aceste rapoarte sunt plauzibile, vor fi protejate.

Este interzisă orice formă de represalii împotriva persoanelor care raportează incidente de fraudă, inclusiv amenințările cu represalii și tentativele de represalii.

Informații detaliate privind protecția identității avertizorului și interzicerea represaliilor împotriva avertizorilor sunt furnizate în **Politica privind avertizorii de integritate și nerepresaliile**.

9) Consecintele incalcarii acestei Politici

Orice încălcare a acestei Politici poate duce la riscuri de răspundere pentru Telekom Mobile și/sau membrii organelor lor corporative și/și funcționarii/angajații acestora și, ulterior, poate atrage sancțiuni disciplinare sau de altă natură împotriva celor care încalcă Politica. Mai mult, orice încălcare a acestei Politici poate avea consecințe juridice negative (penale sau civile, cum ar fi obligația de despăgubire) împotriva Telekom Mobile, precum și împotriva celor care încalcă Politica.

10) Intrarea in vigoare – Modificare

Politica este modificată atunci când se consideră necesar, luând în considerare eficacitatea implementării sale, necesitatea modificării acesteia, precum și posibilele modificări ale cadrului legal și de reglementare.