POLICY	
Title:	**WHISTLEBLOWING & NON-RETALIATION POLICY**
Process Group:	
Process Owner:	**COMPLIANCE DEPARTMENT**
Effective Date:	**17/10/2023**
Summary:	The Policy sets the framework for the adoption of a reporting system in TKRM regarding violations of corporate policies and procedures, regulations and applicable legislation, including breaches of Union law, describes the process regarding the submission, receipt and monitoring of reports and provides an integrated framework for the protection of persons who report breaches related to the above-mentioned matters.

	POSITION	SIGNATURE
Created by:		
Reviewed by:		
Approved by:	Board of Directors of Telekom Romania Mobile Communications Decision 294/17.10.2023	

DOCUMENT REVISION HISTORY		
Version	**Date**	**Description of Changes**
1.0	17/10/2023	Harmonization with OTE Group Whistleblowing Policy Implementation of Law no.361/2022 on the protection of the whistleblower in the public insterest

Contents

1) Preamble

The fundamental principles of transparency, integrity and business ethics govern the operation of TKRM. The Management is committed to ensure that the business activity of TKRM follows the principles of good corporate governance and sustainable development and meets high corporate responsibility standards, while at the same time demonstrating zero tolerance on misconduct, which not only has a financial impact, but mainly damages the reputation of Company and undermines the trust between the company and its stakeholders (e.g. customers, suppliers, employees, shareholders, etc.) as well as other interested parties.

In this context, TKRM adopts an integrated report management system which has at its core the protection of the whistleblowers and enables both employees and third parties to report breaches of legislation and corporate policies which have come to their attention without the fear of retaliation. The adoption of this system contributes to reducing business risk and avoiding financial consequences, leads to the establishment of a corporate culture of open communication and trust and enhances integrity and transparency both inside and outside the company, rendering employees, key enablers in ensuring a sound work environment and socially responsible citizens.

2) Purpose

The Whistleblowing and Non-Retaliation Policy (hereinafter 'Policy'), sets the framework for the establishment of internal reporting channels in TKRM regarding breaches of corporate policies and procedures, regulations and applicable legislation, including breaches of Union law, as laid down in Law no.361/2022- Transposition of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 (L 305) and other urgent provisions'}. Furthermore, the Policy describes the process regarding the submission, receipt, management and monitoring of the said reports and provides an integrated framework for the protection of persons who report breaches related to the abovementioned matters, in order to ensure that they will not suffer retaliation of any kind.

In particular, the Policy aims to:

- inform TKRM employees, as well as third parties and encourage them to report eponymously or anonymously any misconduct or even suspicion of potential misconduct or breach of the policies, procedures and regulations adopted by TKRM, as well as any breach of legislation, including breaches of Union law.

- establish, operate and provide to employees and third parties internal reporting channels in order to submit their reports.
- effectively organize the process regarding the submission, receipt and monitoring of reports, designating a dedicated person as responsible for the receipt and monitoring of reports in TKRM, who shall ensure the prompt and effective response after the submission of the report, manage the report with confidentiality, impartiality and objectivity and provide relevant information to the whistleblower on its progress and completion.
- ensure that employees submitting reports are entitled to protection provided that, at the time of the report, they had reasonable grounds to believe that the information related to the breaches reported was true and to ensure that they will be protected against potential retaliation. Likewise, it aims to ensure the protection of the rights of all persons involved, including the reported persons.

3) Scope

3.1. The provisions of this Policy apply to those working in TKRM and have acquired, in the context of their work, information regarding breaches and in particular:

- to employees, regardless of whether their employment is full or part-time, permanent or seasonal, from the company's premises or remotely or whether they are seconded,
- to persons having self-employed status or to consultants,
- to shareholders and persons belonging to the administrative, management or supervisory body of the company, including non-executive members,
- to any person working under the supervision and direction of contractors, sub-contractors, and suppliers,
- to volunteers and paid or unpaid trainees,
- to persons reporting information on breaches acquired in a work-based relationship which has ended for any reason whatsoever, including retirement, as well as to persons whose work-based relationship is yet to begin, in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

3.2. The provisions of this Policy also apply, as the case may be, to:

- facilitators who contribute to the reporting process in the work-related context
- third parties who are connected with the whistleblowers and who could suffer retaliation in a work-related context, such as colleagues or relatives of the whistleblowers, and
- private companies or legal entities owned by the whistleblowers, or for which the whistleblowers work, or are otherwise connected with in a work-related context.

3.3. The provisions of this Policy apply for the submission, receipt, management and monitoring of the reports regarding breaches of corporate policies, procedures, regulations, codes, circulars, work

directives, as well as of the applicable legislation. The breaches may concern, indicatively and not exclusively, the following:

- breaches of the Code of Conduct, the Supplier Code of Conduct, the Code of Ethics for Senior Financial Officers, the Code of Human Rights and Social Principles, the Internal Personnel Regulation
- incidents of violence and harassment at the workplace, including sexual and gender-based violence and harassment,
- breaches related to human rights issues,
- theft, embezzlement, fraud, active and passive corruption, misappropriation, forgery, property damage,
- falsification of accounting records and financial statements,
- insider trading and market abuse,
- breaches of the legislation and on corporate governance,
- breaches of consumer protection legislation,
- breaches of environmental protection legislation,
- breaches of the legislation on the protection of personal data,
- money laundering and terrorist financing,
- crimes against the security of telephone communications, interference with the operation of information systems, breach of privacy,
- breaches of anti-trust legislation.

In general, the provisions of this Policy apply to any act or omission that may cause a material or non-material damage to TKRM.

If the report includes information on criminal acts or omissions for which legal action is required, it is sent without delay to the Legal Department for investigation and decision making regarding the appropriate legal measures.

Moreover, if from the report or from the other data that may be collected during the investigation process, emerges that there is a serious reason to put the involved employee (or employees) on special leave for as long as the investigation of the case is in progress, so that it can be carried out unhampered, the Human Resources Director is informed immediately in order to take the necessary measures. During the special leave, the employee is removed from duties, but receives the agreed remuneration.

3.4. In particular, the provisions of this Policy also apply to the breaches provided for in Annex 2 of Law 361/2022:

a) breaches of Union law in the following areas:

- public procurement,
- financial services, products, and markets, as well as prevention of money laundering and terrorist financing,
- product safety and compliance,
- transport safety,

- protection of the environment,
- radiation protection and nuclear safety,
- food and feed safety, as well as animal health and welfare,
- public health,
- consumer protection,
- protection of privacy and personal data, as well as security of network and information systems,

b) breaches affecting the financial interests of the Union as referred to in article 325 of the Treaty on the Functioning of the European Union (T.F.E.U.) and as further specified in relevant Union measures,

c) breaches relating to the internal market, as referred to in par. 2 of article 26 T.F.E.U., including breaches of Union competition and State aid rules, as well as breaches relating to the internal market regarding acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

3.5. The application of the provisions of this Policy is not limited by the existence of confidentiality agreements or clauses (e.g. with customers, suppliers, employees, consultants, etc.).

4) Exceptions

The provisions of this Policy do not apply:

- To submit and manage customer or third parties' complaints regarding commercial and technical issues related to company's products or/and services.
- To question business decisions made by TKRM or review/re-evaluate any matter that has already been examined through a disciplinary or other procedure.

5) Definitions

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: TKRM.

Employees: Persons working in TKRM, as defined in paragraph 3.1. hereof.

Report: Oral or written or via an online platform/e-mail communication of information on breaches of this Policy.

Whistleblower: TKRM employees or/and third parties, natural persons, who report information on breaches acquired in the context of their work-related activities, directly or indirectly, with TKRM

Reported Person: Any TKRM employee to whom the breach is attributed.

Retaliation: Any direct or indirect act or omission occurring in a work-related context, which causes or may cause unjustified detriment to the whistleblower, or put them at a disadvantage, related to the provision of information on breaches of this Policy.

Reports Receiving and Monitoring Officer (R.R.M.O.): The natural person designated by the Company as responsible to receive, monitor and manage the reports.

6) 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.

7) Process of submission, receipt, monitoring/management, and completion of the report

7.1. Submission:

TKRM employees or/and third parties, natural persons (hereinafter whistleblowers) may submit written or oral or by e-mail or via an online platform, available on the company's website, also accessible to persons with disabilities, an eponymous or anonymous report, including information on possible breaches that have come into their attention.

The oral report may be submitted by phone or other voice messaging systems, as well as by means of a physical meeting or phone communication with the R.R.M.O. within a reasonable timeframe, upon request by the whistleblower. In case of an oral report, the personnel responsible for handling the report document the oral report in the form of accurate minutes of the conversation, that shall be signed by the author and the whistleblower. In case the whistleblower refuses to sign, an indication is made thereof by the author of the minutes.

7.2. Receipt:

The R.R.M.O. is the person responsible to receive the eponymous and anonymous reports on breaches and acknowledges receipt of the report to the whistleblower within seven (7) working days from the date of receipt. If the report is (i) incomprehensible or (ii) unduly submitted or (iii) there are no serious indications of a breach, the R.R.M.O. may close the case by filing the relevant report without further action, notifying the respective filing decision to the whistleblower. Especially for the breaches mentioned in paragraph 3.4 hereof, the R.R.M.O. informs the whistleblower on their right to re-submit the report, in case they consider that it has not been effectively handled, to the National Agency of Integrity ('A.N.I.') as an external reporting channel, providing them with the relevant contact details.

7.3. Monitoring/Case Management:

The R.R.M.O. follows up on the reports and maintains communication with the whistleblower and, if required, asks further information from them. Furthermore, the R.R.M.O. takes the necessary actions, so that the report is handled, where necessary, by the competent business units of the company, transmitting the report to them and communicates with them in order to be informed on the actions taken to handle the report. The R.R.M.O. informs the whistleblower on the actions taken for the management of their report.

7.4. Completion:

The actions undertaken for the management of the report must be completed within a reasonable timeframe, which does not exceed three (3) months from the acknowledgment of receipt of the report. In case a longer period of time is required, e.g. due to the report's complexity, the whistleblower is informed of the reasons for the extension of the investigation. After completing the investigation of the report, the R.R.M.O. notifies the whistleblower and the reported person, upon their request, of the investigation report. Especially for the breaches mentioned in paragraph 3.4 hereof, the R.R.M.O. informs the whistleblower that they have the right to re-submit the report, if they consider that it has not been effectively handled, to the A.N.I. as an external reporting channel, providing them with the relevant contact details.

As regards the individual actions taken by the R.R.M.O. regarding the receipt of the report and effective case management (e.g., categorization of the reports, plausibility check report, appointment of a case manager, cooperation with other business units, conducting investigations, implementation of measures, etc.), the provisions of the Processes: Compliance Management Process-Tell me! & Compliance Management Process-Case Management shall apply.

8) Internal Reporting Channels

The company has established internal reporting channels which can be used by company employees or/and third parties to address their reports. The below internal reporting channels are available:

- **E-mail address**: available both on the corporate intranet (intranet, shared folder, etc.) and on the website of TKRM : whistleblowing.mobil.ROU02@telekom.ro

- **Electronic Whistleblowing Form** available on the website https://mobile.telekom.ro/about-us/reporting-irregularities/form-reporting/ which enables the submission of an anonymous report. However, in the case of an anonymous report, the breach must be described accurately and in full detail so that it can be investigated.

- **Postal Address**

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

9) Anonymous reports

The R.R.M.O. also receives, manages and monitors anonymous breach reports falling within the scope of this Policy. To this regard, the aforementioned electronic whistleblowing form is available, which enables the submission of anonymous reports. However, taking into consideration that the investigation of the anonymous reports is difficult, their handling is at the discretion of the company. Those who report breaches anonymously must provide full, sufficient, and accurate information to facilitate the

investigation. Persons, who anonymously provide information on breaches and are subsequently identified and suffer retaliation, shall nonetheless qualify for protection pursuant to the provisions of paragraph 13 below.

10) Roles and Duties

10.1. TKRM employees

All TKRM employees, as defined in paragraph 3.1. hereof, are informed at the beginning of their employment or collaboration with TKRM on this Policy and the relevant processes.

TKRM is looking to the integrity of their employees and acknowledge their important role in detecting breaches of corporate policies and procedures, regulations and applicable legislation, including breaches of Union law. Therefore, they should encourage employees to always be alert and report without delay any breach or suspected breach that has come to their attention.

In addition, TKRM is committed to provide and maintain an honest and transparent working environment, where employees feel safe to address their reports in good faith, as well as any concerns they may have, without fear of retaliation.

10.2. Reports Receiving and Monitoring Officer (R.R.M.O.)

The R.R.M.O. shall:

- Perform their duties with integrity, objectivity, impartiality, transparency, and social responsibility.
- Respect and comply with the rules of confidentiality and secrecy for matters of which has become aware in the performance of their duties.
- Refrain from dealing with certain cases, declaring an impediment, if a conflict of interest exists.

10.2.1. R.R.M.O. Duties

In addition to those mentioned in paragraph 7 above, the R.R.M.O. has also the following duties:

- To provide the appropriate information regarding the submission process of a report by company's employees or/and third parties, uploading relative information in a prominent place on the corporate intranet as well as on the company website.
- To ensure the confidentiality of the reports received, as well as the confidentiality of the identity of the whistleblower, of the reported person and of any third party referred to in the report, preventing access to it by unauthorized persons.
- To provide clear and easily accessible information on the process under which reports for the breaches mentioned in paragraph 3.4 hereof can be submitted to the A.N.I. and, where applicable, to public authorities or institutions and other bodies or organizations of the European Union.
- To plan and coordinate training programs and awareness activities on ethics and integrity and to participate in developing internal policies in order to promote transparency and open communication within the company.

- To ensure that the competent personnel involved in case management is properly trained.

10.2.2. TKRM has designated the Head of Legal, Compliance, Data privacy, Environment and ISO Coordinator , as R.R.M.O. who, for the breaches mentioned in paragraph 3.4 hereof, directly reports to the company's Board of Directors.

The term of office of the R.R.M.O. is 5 years and is renewed by a decision of the company's Board of Directors. The term of office can be terminated earlier for an important reason following a decision of the company's Board of Directors.

If the person designated as R.R.M.O. executes at the same time other duties, they must ensure that the execution of these duties does not affect their independence and does not lead to a conflict of interest in relation to their duties as R.R.M.O.

10.2.3. Reports submitted through TKRM internal reporting channels are received by the R.R.M.O., who forwards them to be handled by the competent employees of the business unit responsible to manage the reports, falling under the Head of Legal, Compliance, Data privacy, Environment and ISO (hereinafter 'TKRM Case Management').

If a report is submitted outside the internal reporting channels mentioned in paragraph 8 above, the recipient of the report is obliged to forward it to the R.R.M.O. of TKRM.

10.3. TKRM Compliance Case Management

The TKRM Compliance Unit is an independent business unit within the company, which is supervised by the Board of Directors in order to strengthen its operation and ensure its independence.

In particular, the Compliance Case Management team of the TKRM is staffed by specially trained employees who handle the reports received by the R.R.M.R. and forwarded to them. The competent employees collect and register the reports in a special file/platform, with access rights strictly limited to those responsible to handle the reports.

The responsible employees perform a plausibility check of the report and draft a relevant plausibility check report. If the report is found not plausible, the responsible employees inform the R.R.M.O. in order to close the case as set out in paragraph 7.2 hereof. If the report is found plausible and investigation is required, the responsible employees, in cooperation with the R.R.M.O., inform the competent bodies/business units of the company that need to be informed or take action concerning the report, as set out in paragraphs 7.3 and 7.4 hereof.

The individual actions which are required for the receipt of the report and effective case management are described in detail in the Processes: Compliance Management Process-Tell me! & Compliance Management Process-Case Management.

10.4. Case manager

If the report is found plausible and further investigation is required, the R.R.M.O. appoints a case manager among the employees of TKRM Compliance Case Management.

The case manager has, inter alia, the following duties:

- Carries out the investigation and cooperates, if required, with the competent bodies/business units of the company regarding the actions that must be taken for the effective management of the report.
- Has access to and receives copies of files, data, documents, books, electronic data storage and transfer media, which are necessary for the conduct of the investigation and the verification of the breach.
- Invites in writing the persons involved or other persons to provide information on the breach.
- Drafts a report on the investigation results and proposes measures to sanction the breach, as well as measures to mitigate the risks in the area concerned.

The individual actions required on behalf of the case manager for the effective management of the report are described in detail in the Process: Compliance Management Process-Case Management.

10.5. OTE Group Compliance, Enterprise Risks & Corporate Governance Committee

The OTE Group Compliance, Enterprise Risks & Corporate Governance Committee has as its main purpose the support, control and monitoring the implementation of the Compliance Management (CMS), Enterprise Risk Management (RMS) and Corporate Governance Systems at OTE Group level. To this regard, it assigns responsibilities regarding the carrying out of investigations of compliance related reports, monitors the implementation and completion of the abovementioned investigations (Case Management), appoints 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).

11) Confidentiality and Personal Data Protection

The R.R.M.O. ensures that the reports on breaches of corporate policies and procedures, of the regulations and the applicable legislation, including breaches of Union law are handled with confidentiality and the personal data included therein, pursuant to the provisions of the Regulation (EU) 2016/679 ("GDPR") and Law 190/2018.

11.1. Protection of the identity of the whistleblower and of the reported person

11.1.1. Personal data and any kind of information that leads, directly or indirectly, to the identification of the whistleblower, are not disclosed to anyone beyond the R.R.M.O. and the authorized members of the personnel who are responsible to receive or follow up on the reports, without the explicit consent of the whistleblower. To this end, the company takes the appropriate technical and organizational measures, such as pseudonymization or/and encryption techniques, in handling the report and communicating with the competent bodies/business units of the company, as well as the competent authorities, when required.

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 the context of investigations by

competent authorities or in the context of judicial proceedings, and provided that this disclosure is necessary to safeguard the defense rights of the reported person. In this case, the whistleblower shall be informed in writing before their identity is disclosed of the reasons for the disclosure and the confidential data concerned, unless such notification would jeopardize the related investigations or judicial proceedings. After the notification, the whistleblower has the right to submit in writing their objections and if they are not considered sufficient, the disclosure of their identity and of the other confidential information is not prevented.

11.1.2. Similarly, to the above rules, the identity of the reported persons is also protected throughout the investigation that was initiated following the report. Furthermore, the presumption of innocence applies for the reported persons and they have, inter alia, the rights to be heard and to access their file, provided that the conditions set out in paragraph 11.2 below are met.

11.2. Personal data protection

The processing of personal data when handling the reports under this policy shall be carried out pursuant to the provisions of the Regulation (EU) 2016/679 ("GDPR") and Law 190/2018.

The company is the data controller for the personal data processed and kept in relation to the submitted reports. To this end, the company takes the appropriate technical and organizational measures so 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.

By way of derogation from the relevant GDPR provisions concerning the rights of the data subjects, the company does not provide information to the reported person and to any third party referred to in the report regarding the report, the data included therein and the subsequent processing of their personal data for as long as required and, if it is deemed necessary for the purpose of preventing and addressing attempts to obstruct the investigation, obstruct, cancel or delay monitoring measures, especially regarding investigations, or attempts to identify the whistleblowers, as well as for their protection, informing the subjects (reported person and any third party referred to in the report), upon their request, of the reasons for restricting their rights. In the same context, the Company may not satisfy the rights provided by articles 15-22 of the GDPR and reject (explaining the reasons) relevant requests of the parties involved for the period of time that will be considered critical as set out above.

The transmission to the competent supervisory and investigative authorities of the information included in the reports which can be used as evidence in administrative, civil and criminal investigations and proceedings is permitted.

In any case, the R.R.M.O. must consult the Data Protection Officer (DPO) of the company on any matter that may arise in relation to the processing of personal data of the whistleblower, the reported person or any third party referred to in the report or has occurred during the investigation of the report.

12) Record keeping

The TKRM Compliance Case Management competent employees register in a special file/platform with access rights strictly limited to those responsible to handle the reports, the reports received by the R.R.M.O. In particular, the following information is registered:

- report number, subject matter of the breach, category in which the report falls, origin of the report, date of receipt of the report, brief description of the report and the OTE Group company to which the breach concerns.
- information on the actions taken during the investigation of the report.
- information on the assignment of duties and the timeframe for conducting the investigation
- result of the investigation
- disciplinary or other corrective measures taken.

The reports as well as the relative evidence and personal data included are kept for a period of five (5) years from the completion of the follow up of the report or from the adoption of measures to protect the whistleblowers or the adoption of disciplinary measures or/and legal actions against the reported persons or third parties and in any case until the completion of any investigation or judicial proceeding initiated as a result of the report against the reported person, the whistleblower or third parties.

The Company may retain the personal data after the abovementioned period in the following limited cases: (a) if this is necessary and for as long as it is required in the context of pursuance of the processing purposes, or (b) if there is a legal obligation from a relevant law provision, or (c) for defending the rights and legitimate interests of the Company before any competent Court and any other public authority within the provided limitation period.

Personal data is exclusively stored at company's premises, where it is protected by appropriate security measures and is not transmitted to third countries outside the European Economic Area (EEA).

13) Protective Measures – Non-Retaliation

13.1. TKRM takes all necessary measures to ensure that persons providing information about breaches of corporate policies and procedures, regulations and applicable legislation, including breaches of Union law, believing reasonably and in good faith that these reports are plausible, will be protected.

The company, if required, provides free psychological support to whistleblowers.

Without prejudice to law, the whistleblowers shall not incur, inter alia, liability in relation to (a) the acquisition of information or access to information reported, provided that such acquisition or access does not constitute a self-standing criminal offense, and (b) the reports themselves, if they have reasonable grounds to believe that the report was necessary to reveal a breach.

Any form of retaliation against the persons mentioned in paragraphs 3.1 and 3.2 hereof is prohibited, including threats of retaliation and attempts of retaliation.

In particular, the following forms of retaliation are prohibited:

a) suspension, dismissal or other equivalent measures,

b) demotion, omission, or withholding of promotion,

c) removal of duties, change of location of place of work, reduction in wages, change of working hours,

d) withholding of training,

e) a negative performance assessment or employment reference,

f) reprimand, imposition of disciplinary or other measure, including a financial penalty,

g) coercion, intimidation, harassment, or ostracism,

h) discrimination or unfair treatment,

i) failure to covert of a temporary employment contract into a permanent one,

j) failure to renew or early termination of a temporary employment contract,

k) intentional harm, including to the person's reputation, particularly on social media, or financial loss, including loss of business and loss of income,

l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry.

m) early termination or cancellation of a contract for goods or services,

n) revocation or cancellation of a diploma or license,

o) psychiatric or medical referrals,

p) denial or deprivation of reasonable accommodation to disabled persons.

13.2. In case of retaliation, the persons against whom retaliation was undertaken, are entitled to full compensation for the damage suffered and may request the things to be restored to the state they were before the retaliation, if this is objectively possible and not disproportionately onerous for the Company. The termination of an employment contract that takes the form of retaliation, is in any case void.

13.3. Exceptionally, no protection is provided to whistleblowers when they make a false and malicious report, being aware of the untruth of the allegations, aiming to harm the reported person or benefit themselves. The knowingly submitted false report on behalf of the employees may lead to the imposition of disciplinary measures by the Company, not excluding the right to terminate the employment contract.

14) Legal Consequences

Any violation of this Policy may result in liability risks for TKRM or/and the members of their corporate bodies or/and their officers 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 TKRM, as well as against those violating the Policy.

15) Entry into force – Amendment

This Policy enters into force for TKRM by a decision of its Board of Directors.

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. In case of any necessary amendments of the Policy, the provisions of the PL1.EEM.01 Policy (Approval of Corporate Policies / Processes / Procedures" regarding the CMS Policies) shall apply.

This Policy repeals Whistleblowing Policy as of 23.05.2017 which is fully terminated on the entering in force of this Policy.