office@next-gen.ro
www.next-gen.ro

POLICY	
Title:	**ANTI - FRAUD POLICY**
Process Group:	**ENTERPRISE RISK MANAGEMENT**
Process Owner:	**COMPLIANCE DEPARTMENT**
Effective Date:	**08/08/2018**
Summary:	This Policy provides a description of the rules and the basic guiding principles with regard to the fraud incidents that may occur at OTE Group companies and it sets the necessary measures for the prevention of such fraud cases.

	POSITION	SIGNATURE
Created by:	Alina Rebeca MUSAT - Compliance Expert	
Reviewed by:	Claudia PETRE - Compliance Director	
Approved by:	Norbert Ulysse HOECKL - Executive Director Administrative and Development Andrei Stefan CRETU – Chief Executive Officer	

office@next-gen.ro
www.next-gen.ro

DOCUMENT REVISION HISTORY		
Version	**Date**	**Description of Changes**
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 NextGen Communications Updates according to current Organizational Chart

office@next-gen.ro
www.next-gen.ro

Contents

office@next-gen.ro
www.next-gen.ro

1) PREAMBLE – SCOPE

The offense of fraud, also known as "white-collar" crime, is of particular concern to companies. In several cases, the offenders are from the company's own environment. The aforementioned offense may primarily result in severe economic losses/damages for the companies in which it occurs. Often these losses are related to other equally significant damages, such as to the company's reputation, as the latter has been formed in both the investors' and the general public's ranks as well as in the relationships with business partners.
Taking preventive measures for the identification of risks and acting consistently against "white collar" crimes present therefore permanent challenges and are important components of a responsible corporate policy.

At NextGen Communications S.R.L. (hereafter "NextGen Communications" or "Company"), as in the entire OTE Group, "white collar" crimes and similar misconduct are not acceptable.
This Anti-Fraud Policy (hereinafter referred to as "the Policy") is established to facilitate the development of control mechanisms and safeguards that will aid in the detection and prevention of fraud against OTE Group companies.

Specifically, the objective of the Anti-Fraud Policy is to create a group-wide framework which should ensure:

- That anti-fraud and anti-bribery programs and control mechanisms are effective in preventing, detecting and pursuing fraud and bribery incidents;
- Achievement of high levels of business integrity through proper and effective corporate governance, internal control mechanisms and transparency.

The OTE Group companies count on the integrity of their employees and recognize that they have a key role in the prevention, detection and reporting of fraud and bribery. Therefore, the employees are asked to be vigilant at all times and to report immediately any suspicion they may have.

At the same time, the OTE Group companies are committed to the existence and maintenance of honest and transparent working environment, where the employees are confident to report their suspicions without fear of reprisals.

Anti-Fraud and Anti-bribery Management is an integrated component of the OTE Group-wide Compliance Management System and part of its corporate culture.

The Policy presents the basic principles and elements of the OTE Group's anti-fraud and anti-bribery management and contains instructions and recommended actions for handling cases of fraud and bribery. Furthermore, the aim of this Policy is to help all OTE Group business units to take the necessary measures to prevent and combat fraud and bribery, and to support efforts by OTE Group employees at all levels to defend themselves against risks caused by fraud and bribery incidents.

Finally, this Policy should contribute to promoting dialogue and sensitization at all management levels regarding fraud issues and increase the awareness regarding the problems caused by fraudulent behavior in general.

2) AREA OF APPLICATION

2.1 In this Policy, OTE Group is defined as OTE S.A. and OTE's affiliated companies. Any reference to a "Company" made in this Policy means any company of the Group. This Policy applies to all OTE Group companies, including NextGen Communications S.R.L. (hereafter "NextGen Communications" or "Company").

2.2 This Policy applies to any fraud incident or indications for fraud perpetration, which could lead to financial losses or/and increase the reputational risk of NextGen Communications company, involving:

- persons employed at the Company with employment contracts or loaned employees or in-house attorneys (hereinafter referred to as "Personnel"),
- persons employed at the Company as independent contractors or providers of independent services on the basis of any contractual relationship, e.g. temporary employment companies or collaboration companies' staff, Partners, Startups (hereinafter referred to as "Partners"),
- third parties, physical or legal entities with which the OTE Group companies collaborate (e.g. suppliers, customers) or maintain a business relationship,
- BoD members, CEOs Chief Officers as well as executives up to the hierarchical level of Section Manager of the Company (hereinafter referred to as "Management").

The term "Employees" includes the Company's both Management and Personnel.

2.3 Any investigative activity required will be conducted without regard to the length of service at the Group of the person alleged to have been involved or/and kind of the employment or/and position/title or relationship with the Company.

3) ACCESS RIGHTS

This Policy is made available on the Process Web and is accessible to all Employees / Partners. Dispatch of the Policy outside the Company is not permitted.

4) DESCRIPTION – KINDS OF FRAUD

In the context of and for the purpose of this Policy, fraud is defined as any act, omission or act of tolerance by Employees or Partners or third parties with the knowingly representation of false facts as true or the unfair disclosure or concealment of true facts, for the purpose of personal gain or to induce injury or financial loss.

Fraud in the above sense may consist or/and also imply any breach by Employees or Partners or third parties of both the legislation in force and the Capital market–related provisions, as well as the internal processes, regulations, circulars and policies which have been adopted by the Company and which may result in adverse economic and/or other impacts on the Group.

Acts that may constitute fraud are, in the context of the abovementioned definition, among others:

- Fraudulent misrepresentation of facts
- Disguise of facts
- Concealment of true facts
- Breach of official duty
- Perjury
- Forgery
- Blackmail
- Capital investment deception
- Theft and Embezzlement
- Falsification of documents and other relevant actions
- Falsification of company records
- Manipulation of accounting and financial statements
- Destruction, removal of records, furniture, fixtures, and equipment
- Manipulation of rate or market price of the Company (in case of listed companies)
- Corruption and/or active and passive bribery (pursuit of uncanny personal gain, granting advantages, receiving or giving bribes)
- Economic extortion
- Concealment of hiding of conflicts of interest
- False claims and statements to government agencies
- Insider trading
- Cyber crime

- Counterfeiting of products and brand piracy
- Misuse of private or business secrets
- Anti-competitive agreements/cartels
- Money laundering
- Violation of the Procurement Policy
- Violation of the Purchases/Expenditure Policy
- Violation with intent of the Company's legal representation rules including signature rights

5) BASIC PRINCIPLES

NextGen Communications encourages all Employees, Partners and third parties to feel confident in reporting incidents of fraud and fully understands their important role in developing a culture for preventing, detecting and taking corrective actions for the prevention of fraud.
Any fraudulent behaviour or other irregularities, which are detected or suspected, must be reported immediately by Employees / Partners, using the channels of communication offered by NextGen Communications mentioned in article 5.5.1 of this Policy.
If there is any doubt about the existence of sufficient indications of suspected fraud, the contacts to be named, in accordance with paragraph 5.3.1. of this Policy, will provide advice and assistance in assessing facts.

5.1) Responsibilities

The Company's Management is responsible for taking measures aiming to prevent and detect fraud and other irregularities in business areas and its internal operation.
Nevertheless, it should be understood that Employees / Partners have different roles and responsibilities with respect to fraud prevention, detection and deterrence and must always comply with the national laws.
In case of doubt about applicability, validity and sanctions of the existing legal framework provisions, the Legal Department must be consulted.
The Company's Management must perform their duties by observing the principles of due professional care, which is reflected in the following organizational duties at a minimum.

5.2) Organizational Duties

The Company's Management will:

- Ensure of the establishment of clear organizational structures and responsibilities;
- Guarantee clearly defined responsibilities and compliance with appropriate principles of proper delegation of tasks and obligations ("segregation of duties");

- Ensure proper selection, briefing (training/giving information) and monitoring of Employees, Partners and third parties;
- Ensure obtaining and complying with legal advice provided by the Legal Department;
- Allocate tasks according to responsibilities and expertise of the Employees / Partners and oversee the compliance of the Company's representatives' individual decisions with the dual control principle ("4-eyes principle");
- Ensure that representation, signature and approval limits rules are clearly established;
- Monitor compliance through internal and external audits;
- Ensure that any fraud cases that occur are reported to the competent bodies at regular intervals and ad hoc whenever necessary.

When delegating tasks, the following principles should be adhered:

- Proper selection of Employees, Partners and third parties according to their expertise;
- Regular monitoring of specialized knowledge and the reliability of Employees, Partners and third parties as well as evaluation of them;
- Regulated delegation of duties and responsibilities at lower hierarchy levels;
- Rationalism as to the requirements on Employees / Partners entrusted with responsibilities;
- Giving clear and comprehensive instructions;
- In the event of misconduct by Employees / Partners entrusted with responsibilities, prompt investigation, consequence management and elimination of deficiencies is required.

5.3) Measures

5.3.1) Contacts for Anti-Fraud Management

Depending on the tasks and size of the Company, the Company will designate the persons competent for anti-fraud management and will inform the Employees / Partners appropriately.

5.3.2) Risk Analysis & Fraud Risk Assessment

An important condition for an effective and efficient fraud deterrence program is the systematic recording and analysis of fraud risks within NextGen Communications (Compliance & Fraud Risk Assessment).
Fraud Risk Assessment will be carried out by the responsible business units, i.e. Compliance department together with IT Department, Administrative Department and Internal Audit if necessary, in order to identify potential fraud risks in specific areas of operation (e.g. Sales, Procurement, Accounting).
This assessment, which will take place at regular intervals and/or whenever necessary, will present which control mechanisms exist for the prevention and detection of fraud and will

determine any additional necessary measures for the reduction or elimination of identified fraud risks. The Fraud Risk Assessment should take into consideration the fraud cases which have been reported in the past.
The responsible business units will update the relevant questionnaires, organize workshops, centralize results and monitor the implementation of relevant measures.

5.4) Fraud Prevention

NextGen Communications promotes awareness of fraud prevention or treatment among Employees and Partners.
All Employees and Partners will be informed, at the time of employment, on this Policy and on issues of fraud, including risks and sanctions for committing fraud. Furthermore, relevant updates will be provided each time a new particular risk factor is detected.
Employees or Partners working in sensitive departments or units that are exposed to higher fraud risks will receive, at regular intervals, more in-depth training focused on fraud regarding their assigned responsibilities

5.4.1) Selection and Placement of Employees / Partners

The reliability and personal integrity of Employees / Partners is an important factor in the reduction of fraud risk.
The Company's applicable recruitment process is designed to facilitate a consistent assessment of the reliability and integrity of the candidate, beyond the professional suitability. In this respect, the applicable internal processes for checking the candidates are applied. Endorsement from Compliance should be obtained when a potential/real conflict of interest is declared by a candidate. Also, periodical performance evaluation should re-consider the suitability of the Employee / Partner for the performance of the same tasks.

In particular, careful attention should be paid to the suitability of applicants in terms of reliability and integrity as well as professional competence, when filling positions in job areas in which the Fraud Risk Assessment has revealed that the Employee's / Partner's performance of the same tasks over time, increase fraud risk factors. In these areas, a periodical change of Employees' / Partners' tasks should also be considered as a possible tool for reducing fraud risks.
When considering a periodic change of tasks, the Employee's / Partner's personal issues (marital status, maternity leave, sickness, etc.) should be taken into account as far as possible, in particular as regards the timing of the change of tasks.

5.4.2) Organizational Control Mechanisms

NextGen Communications promotes transparency in business decision-making.

When performing transactions with third parties, written and detailed documentation is required, which will accompany the transactions and will give a full and precise account of the individual steps until the completion of a transaction. The significant transactions must be documented, as the law or/and the Company's Policies / Procedures provide, and must be archived in a suitable form.

Fraud prevention safeguards in transactions as well as suitable transaction control mechanisms must be planned in the business processes. These mechanisms serve to protect Employees / Partners and ensure the detection of fraud.
In areas in which the Fraud Risk Assessment has revealed an increased risk of fraud, particularly strict control measures are required and the execution of these measures should be documented in writing such that they can be traced.

Organizational measures, mostly drafting processes on responsibility, should be taken in order to minimize fraud risks. These measures should apply the principle according to which more than one persons are required to participate in the decision making process ("4-eyes principle"). This can be implemented through the allocation of decision-making responsibilities along with the extending and strengthening of control mechanisms.
The application of the "4-eyes principle" and the "segregation of duties" should be encouraged, where possible.

5.5) Fraud Detection

If there are specific indications of fraud, the case will be investigated further, so that the investigation will show both aggravating and mitigating circumstances relating to the person involved with fraud, without regard to the person's authority, title or position in the Company.
In this respect, NextGen Communications Romania company will apply the following measures of fraud detection:

5.5.1) Disclosure Duty with Regard to Fraud Incidents and Informing Committees

When Employees and Partners during the execution of their duties and third parties during their cooperation with the Company become aware of incidents which may be considered as indication of fraud or fraud, are obliged to report these to the competent business unit of Compliance using the following Whistleblowing channels:

- **Via Post**:
- Compliance Department, Baneasa Business Technology Park, Sos. Bucuresti-Ploiesti no. 42-44, Building A, Wing A2, Et. 2, 013696, district 1, Bucharest
- **Via e-mail**: raportare.nereguli@next-gen.ro OR

- **Via the Electronic Whistleblowing Form** (available on the corporate website and on our company intranet)

Employees / Partners must also inform their immediate superiors. Subsequent to this notification, NextGen Communications Compliance Committee is informed. In the following cases the Executive Director Compliance ERM and Insurance OTE Group is informed:

- The person involved is a member of the Board of Directors, or a senior executive of the Company.
- The material damage is more than **€ 10.000**
- The tip off regards a matter which could affect the financial statements of the Company or the Group.
- The tip off regards significant immaterial damage, which affects the Company's reputation.

Thereafter, if the estimated material damage is more than **€100.000**, the NextGen Communications Compliance Committee informs the NextGen Communications Audit Committee and, in serious cases (where the estimated material damage is more than **€500.000**, or the person involved is a member of the Board of Directors or a senior executive), the NextGen Communications Board of Directors is also informed.

5.5.2) Responsibilities and Procedure for Investigation

The investigation of suspected fraudulent acts lies exclusively with the business units/persons responsible according to the delegation of responsibilities in the Company, such as in cases of telecommunication fraud, theft by third parties, etc.

The NextGen Communications Compliance Committee (hereinafter referred to as "the Committee") is obliged to delegate responsibilities regarding investigations of tip-offs about fraud or non-compliance with the provisions of law or Policies and processes adopted by the Company, to monitor the implementation and completion of investigations and shall be entitled to propose appropriate sanctions or measures to the respective competent business unit, in case of misconduct, as part of the Compliance Management System. The Committee is entitled to propose corrective measures and measures to limit fraud.

In order to accomplish its mission, while conducting the investigations or other actions, the Committee has the right to address and request the collaboration and participation of Employees / Partners or to hire external consultants, when required.

In the interest of a uniform process of handling cases which are included in the abovementioned categories of paragraph no.4 (Description – Kinds of Fraud), the following principles should be observed:

a) The verification process of facts in order to prove the personal liability of the person involved should not extend beyond the absolutely necessary limit. Further investigation by the competent police or judicial authorities should not be impeded in any way.

b) In cases involving a fraud incident directly related to the performance of work duties or the breach of duty by the Employee, the Legal Department and Human Resources Manager should be consulted at an early stage. The competent bodies of the Companies will decide on the enforcement of appropriate measures (e.g. sanctions, indicatively initiation of disciplinary procedure, termination of contract, etc.).
c) All the investigation steps and the outcome must be documented in writing. For the purpose of the investigation and the detection of evidence, the documentation should be aligned with the control measures and the procedures outlined in the Group Policies and the Compliance Management System.
d) The Legal Department will assist the competent bodies of the Company in the investigation procedures, considering whether the conditions of law are fulfilled for reporting to the Authorities, based on the findings of investigation implemented by the Company's competent units, in accordance with the above. Cases which were not deemed valid by the competent units as well as cases which the prosecuting authorities have undertaken are excluded. Without prejudice to the special investigation of each case, appealing to Authorities should be carried out, indicatively, in cases wherein through fraudulent behaviour, there is damage to the Company's or the Group's assets.
e) Communication with the Authorities with regard to the perpetration of fraud incidents will be carried out by the Legal Department or, in agreement with the Department, by the Company's Compliance Manager.

While conducting the investigation, the executives responsible for the investigation should have, to the extent permitted by applicable law, particularly that on personal data, and the Company's Policies, particularly the Security Policies:

- Free and unrestricted access to all Company records, IT systems and premises, whether owned or leased.
- The authority to examine, copy, use all or any part of the contents of files, desks, cabinets, and other storage facilities on the company's premises, without prior knowledge or consent of any individual who might use or supervise any such items or facilities.

5.5.3) Complaints – Protection of the Person Involved and Confidentiality

Anonymous complaints are more difficult to confirm and, therefore, their investigation is subject to the discretion of the relevant Group Company. In this context, the following factors should be taken into consideration:

- The seriousness of the issue raised.
- The likelihood of confirming the allegation from independent and reliable sources.

The provisions in existing legislation regarding the rights of the person involved should be observed and applied accordingly, during the investigation procedure.

The gathering of evidence must take place using only legally permissible means. If there is any doubt as to the legal validity of individual investigatory measures, the Legal Department must be consulted.

During the period of investigation, the executives responsible for the investigation should refrain from any action which is not part of the verification of facts and which could result in the disclosure of the person(s) involved to third parties.
This applies in particular to written or electronic correspondence between the business unit responsible for the verification of facts and other business units and persons, as well as during the questioning of witnesses. Where a personal description of a person involved or the description of suspicious circumstances he/she is accused of is necessary, it must be made clear that only the suspicion of the perpetration of fraud is in question and the investigation should not extend to other aspects of the involved person's personal or professional life.
Personal data must be handled according to both the applicable law (national and European) on personal data protection and the relevant NextGen Communications companies' regulations.
Persons and business units which can prove they have a justified (legitimate) interest, they can receive information about the existence of any suspicious behaviour and/or the investigation progress or results, provided that this is not prohibited by the existing legal framework.

5.5.4) Whistle-blower Protection

The basic principle is that any information concerning suspected fraud is treated confidentially. If messages are sent via the Electronic Whistleblowing Form (EWF), the confidentiality regarding the identity of the whistle-blower is guaranteed.
NextGen Communications shall take all necessary and reasonable measures to guarantee that persons who provide information on suspected fraud cases, in good faith and having reasonable grounds for believing the information provided is reliable, do not suffer any personal, business or pecuniary loss.

5.6) Fraud Sanctioning

Deliberate misconduct or omissions that violate the present Policy shall be subject to sanctions in accordance with the Company's existing regulations (e.g. Labour Regulation) and labour or criminal law, in general.

5.7) Information about Detected Fraud Cases and Constant Monitoring

The Management will be informed regularly of Fraud Risk Assessment results (fraud risks areas, existing measures, supplementary measures, status of implementation of supplementary measures) and the fraud cases identified together with investigation results and measures taken to deter future fraud from happening.

Any notification of the fraud cases detected will take place, provided that it is permitted by the current legal framework and only through the responsible Marketing Department, following prior agreement by the Legal Department.

The process of internal verification of facts and the process of investigation by the criminal prosecution authorities must not be jeopardized by any notification.

The business units responsible for anti-fraud management will check the quality of processes for handling fraud cases at regular intervals or upon request.

6) ENTRY INTO FORCE & REVIEW OF THE POLICY

This Policy enters into force through the approval of the Company's management. As regards the rest OTE Group Companies, the Policy enters into force by a decision of their competent bodies.

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.