NetWorks

Internal Reporting Regulations

I. Purpose and scope:

The Regulations define the internal procedure for reporting violations of the law and taking follow-up actions used in N. The purpose of these Regulations is to define the rules applicable in N:

- reporting breaches of the law referred to in the Act (being in this respect the rules of internal reporting),
- report breaches of law other than those referred to in the Act, i.e. breaches of the Compliance principles and the Code of Ethics,
- follow-up,
- consultation with the Compliance Officer.

With respect to violations of law referred to in the Act, the provisions of the Act shall apply, which in such a case is a document superior to these Terms and Conditions, including in particular to the extent not regulated in the Terms and Conditions. For the avoidance of doubt, the Regulations do not extend the application of the provisions of the Act beyond the scope of the Act specified therein.

The Regulations apply to all Employees and Associates of N. Each candidate for an Employee and Associate of N is familiarized with the content of the Regulations along with the commencement of recruitment or negotiations preceding the conclusion of the contract.

II. List of definitions, terms and abbreviations:

With regard to reports of breaches of law referred to in the Act, the terms used in the Terms and Conditions and defined in the Act should be understood as defined in the Act. In addition, these Terms and Conditions introduce the following definitions of the terms used:

Compliance – the Compliance Management System, activities aimed at ensuring that all business activities of N are in accordance with the applicable law and internal regulations;

Compliance Officer – a person (internal entity) responsible for compliance issues in N, authorised in writing in the form of a power of attorney by the Management Board of N, to receive and verify internal reports (hereinafter referred to as the "report"), to take follow-up actions, to keep a register of internal reports and to process personal data of persons making reports and persons to whom the reports relate, as well as obliged to maintain secrecy in the above-mentioned scope;

DCS – Cybersecurity Department;

DHR – Human Resources Department;

DPiWB – Legal and Business Support Department;

Compliance channel – one of the channels in accordance with points 6.1.1 and 6.1.2. Code of Ethics;

Code of Ethics – the NetWorks Code of Business Ethics;

N, Employer – NetWorks sp. z o.o. with its registered office in Warsaw;

Employee – a natural person performing work for N on the basis of an employment contract;

Register – a register of internal reports referred to in the Act, created on a dedicated network drive N, ensuring the security and confidentiality of the data collected therein against access by unauthorized persons;

Terms and Conditions – these "Internal Reporting Regulations";

Whistleblower – a natural person who is defined by the Act as a whistleblower, including Employee and Associate N;

Act – Act of 14 June 2024 on the Protection of Whistleblowers

Owner – Orange Polska S.A. or T-Mobile Polska S.A.;

N Associate – a natural person who is not an Employee and who takes action on the basis of a legal relationship other than an employment contract, constituting the basis for the provision of work, services or performing functions in or

for N, where the party to the legal relationship is N, the Owners or contractors, subcontractors or suppliers of N, including persons other than Employees listed in Article 4 of the Act.

III. Role and Responsibility:

1. Compliance Officer

1.1. Within the scope of these Rules, the Compliance Officer acts independently and is responsible for:

- accepting applications,
- communication with the Whistleblower, including requesting additional information and providing feedback to the Whistleblower,
- maintaining the Register on behalf of N,
- verification of applications,
- taking follow-up with due diligence
- providing consultations on violations of the law, compliance principles and the Code of Ethics,
- management of Compliance Channels,
- periodically informing N Employees and Associates about the possibility of making internal and external reports,
- ensuring that reports are handled in a manner that prevents unauthorized persons from gaining access to the information covered by the report and ensures the protection of the confidentiality of the identity of the Whistleblower, the person to whom the report relates, and the third party named in the report, including taking into account appropriate technical and organizational solutions to ensure that the Whistleblower's personal data is stored separately from a document or other information carrier, including including, where appropriate, the removal of all personal data of the reporting person from the content of the document or other information medium immediately upon receipt.

1.2. The compliance officer shall have the right to:

- demand all forms of support during the verification of reports and follow-up actions from other organizational units of N,
- transfer, depending on the type of report, the case to be clarified by another organizational unit N,
- access, control and request information covered by the scope of work from all organizational units of N, except for classified information within the meaning of the Act on the Protection of Classified Information or other information excluded by law,
- prepare copies and extracts from documentation (within the limits resulting from the protection of personal data and with the exception of information of the scope specified in the Act on the Protection of Classified Information and its implementing regulations or other legal provisions), inspect and secure items owned by N or used by N during the verification of reports and follow-up actions,
- during the verification of notifications and follow-up actions carried out, access to the content of messages and to the processing of transmission data concerning messages made with the use of hardware, software and data made available by N within the limits provided for by law, internal regulations of N and only in justified cases,
- access to the controlled area/rooms, carried out in consultation with the person responsible for a given area, in special cases, access is carried out in direct cooperation with DCS, and in the case of DHR in the presence of a DHR employee,
- after receiving the report, to verify the report and take follow-up actions, collect and process the personal data of the person to whom the report relates, even without their consent, and the Whistleblower's data allowing to determine their identity are not disclosed to unauthorized persons, unless with the Whistleblower's express consent or in the cases specified in the Act.

1.3 The Compliance Officer is obliged in particular to:

- perform the tasks entrusted to him or her due and diligent, including the related processing of personal data in a manner that prevents access to the information covered by the notification unauthorised persons and ensuring the protection of the confidentiality of the identity of the Whistleblower and the person to whom the report relates and the person assisting in making the report and the person associated with the Whistleblower – to the extent described in the Act,

- impartial verification of reports,
- confidentiality to the extent specified in the Act,
- take action in accordance with the Act and ensure compliance with the Whistleblower protection rules set out in the Act.

2. Management Board of N

2.1. The Management Board of N authorizes the Compliance Officer in writing to receive and verify internal reports, take follow-up actions and process personal data of persons as part of a given report.

2.2. In the event of a suspicion of committing a crime, the Management Board of N decides whether to report the case to law enforcement authorities or competent public administration bodies.

3. Employees and Associates of N have the right to report a violation of the law, compliance principles and the Code of Ethics through the Compliance Channels.

4. N1 Director, to whom the audited organizational unit N is subordinate, is responsible for supervising the timeliness and quality of implementation of recommendations and recommendations from the follow-up activities.

IV. Description of the procedure:

Introductory remarks:

- A whistleblower is subject to the protection provided for in the Act if he or she had reasonable grounds to believe that the information about the violation of the law referred to in the Act being the subject of the report is true at the time of reporting and that such information constitutes information about a violation of the law. This protection also extends to other persons indicated in the Act to the extent specified therein.
- In addition, under these Terms and Conditions, N ensures that no retaliation may be taken against a Whistleblower who had reasonable grounds to believe that the information about the violation of the Compliance rules or the Code of Ethics being the subject of the report was true at the time of making the report. The above protection extends to the Whistleblower, persons assisting them in making a report, persons associated with the Whistleblower and legal persons or other organisational units associated with the Whistleblower, in particular those owned by the Whistleblower or employing them.
- The Whistleblower's personal data and other data allowing to determine the identity of the Whistleblower, the person to whom the report relates and the information covered by the report are protected in terms of confidentiality and are not subject to disclosure. With the express consent of the Whistleblower, their personal data or other data allowing their identity to be determined are disclosed. The confidentiality protection referred to above applies to information on the basis of which the identity of such persons can be directly or indirectly identified.
- Both the source of the information and the information contained in the report are protected against unauthorized access. In the event of a breach of the law referred to in the Act, the confidentiality of the identity of the Whistleblower and the person to whom the report relates is protected. Confidentiality applies to information from which the identity of such persons can be directly or indirectly identified. For other reports, at the express request of the Whistleblower, reasonable confidentiality protection will also be ensured.
- Personal data processed in connection with the receipt of the application are stored in the Register for a period of 3 years, after the end of the calendar year in which the follow-up actions were completed, or after the end of the proceedings initiated by these actions.
- The provisions of the Terms and Conditions also apply to reports enabling the identification of the Whistleblower and to anonymous reports.

1. Receipt of the application

1.1. A report of violations of the law, compliance rules or the Code of Ethics may be submitted to N in any of the following ways:
   a) through the Compliance Channel (also as an anonymous report),
   b) the Compliance Officer's own observations and findings,
   c) an order from the President of the Management Board of N or a Member of the Management Board of N,

d) mandate from the Supervisory Board of N or its Committees,
e) order from the Compliance Officers of the Owners,
f) by means of a direct meeting with the Compliance Officer organised within 14 days from the date of receipt of the Whistleblower's request for such a meeting. A protocol is drawn up from such a meeting.

1.2. Within 7 days from the date of receipt of the report, the Compliance Officer confirms receipt of the report to the reporting person, unless the Whistleblower has not provided an address to which the confirmation should be sent.

1.3. Anonymous reports are subject to the same rules of conduct as all other reports referred to in the Regulations, unless it is not impossible to clarify the circumstances indicated in the report due to the lack of the Whistleblower's details or contact with them.

2. Registration of the application

2.1. Each report is subject to entry in the Register, which is kept by the Compliance Officer on behalf of the Employer.

2.2. The following data relating to a given report are subject to entry in the Register, i.e.: case number, subject of the breach (indicating whether it is a violation of the law referred to in the Act or another violation), personal data of the Whistleblower and the person to whom the report relates, necessary to identify these persons, the Whistleblower's contact address, the date of the report, the manner and form of the report, information on the follow-up actions taken, the date the case was completed.

2.3. The administrator of the data collected in the Register is N.

2.4. The data in the Register are stored for a period of 3 years, after the end of the calendar year in which the follow-up actions were completed or after the end of the proceedings initiated by these actions.

3. Verification of the application

3.1. After registering the report, the Compliance Officer conducts an initial impartial verification of the report in terms of:

- assessment of the veracity of the allegations contained in the report, the irregularity to which the report relates, including determining whether the report concerns information on the violation of the law referred to in the Act,
- possible risk for N and the Owners (e.g. violation of the law, internal regulations, Code of Ethics, loss of reputation, etc.).

3.2. The Compliance Officer may request clarification or additional information from the Whistleblower regarding the information provided that may be in their possession using the address indicated by the Whistleblower as the contact address. If the Whistleblower objects to the sending of the requested explanation or additional information, or the sending of such requests may jeopardize the protection of the person's identity, the Compliance Officer refrains from requesting clarification or additional information.

3.3. Subject to the provisions of the Act, on the basis of the verification referred to in section 3.1 above, the Compliance Officer makes an impartial decision to:

a) commencement of follow-up actions, which it carries out in accordance with point 4 below, and this always takes place in the case of reporting violations referred to in the Act,
b) abandonment of proceedings, if the notification does not concern N or the Owners or is unfounded,
c) forwarding the notification to the Owners or to TMPL or OPL, respectively, if the notification concerns them,
d) forwarding the report to the appropriate organizational unit in N, if the report does not concern a violation of the law, compliance issues or the Code of Ethics, but concerns organizational matters within a given unit,
e) when the report is forwarded to the Ethics and Compliance Management Committee, then further proceedings are carried out in accordance with the Procedure "Principles of Operation of the Ethics and Compliance Management Committee".

3.4. The Compliance Officer does not follow up if a report on a matter that is already the subject of an earlier report does not contain material new information on the breaches compared to the previous report. In such a case, the Compliance Officer records this fact together with the justification in the Register.

4. Follow-up

4.1. The Compliance Officer carefully and impartially analyzes the report referred to in section 3.3.a) above using the means described below to verify information about breaches of the law, compliance principles or the Code of Ethics, and then determines the scope of work to be performed as part of the investigation.

4.2. Various inspection techniques and measures may be used as part of the investigation, depending on the issue under consideration. These include in particular:

a) interview with an Employee, Associate N,

b) analysis of documentation, transactions and entries in books and any auxiliary databases,

c) analysis of the results of activities and documents related to the ongoing investigation,

d) observation of activities performed by Employees, Associates N,

e) analysis of data contained in IT systems,

f) other analytical techniques.

4.3. The Compliance Officer may request the manager of the organizational unit in N covered by the investigation to prepare reports from IT systems necessary for the proceedings, copies or extracts of documents, as well as statements and calculations made on the basis of these documents.

4.4. The Compliance Officer analyzes the evidence collected in the course of the investigation.

4.5. Violation of the law, compliance principles or the Code of Ethics by an Employee constitutes a breach of employee duties, for which the Employee may be held liable for disciplinary or material liability provided for in the relevant provisions of law and applicable internal company acts. The amount of sanctions for breach of employee duties depends, in particular, on the type of breach of employee duties, the degree of the employee's fault or the consequences of the breach. The employee may also be required to redress the damage resulting from this violation. N's co-workers who are not in an employment relationship with N are liable for violations in accordance with the general rules provided for in the relevant provisions of law.

4.6. In the event of disclosure in the course of the investigation of circumstances justifying the suspicion of committing a crime, the Compliance Officer is obliged to inform the Management Board of N. Without undue delay.

5. Closing of the investigation

5.1. Report on the investigation:

a) Upon completion of the investigation, the Compliance Officer prepares an impartial preliminary report containing a description of the collected evidence and information, conclusions, recommendations and recommendations.

b) Conclusions from the investigation must contain unambiguous assessments and a position on the causes, circumstances, and identification of persons responsible for violating the law, compliance principles or the Code of Ethics. If unambiguous assessments and positions are not possible to issue and take in connection with the evidence collected in the course of the investigation, such information must be provided with a justification.

c) If, in the course of or as a result of the explanatory proceedings, circumstances are revealed justifying recommendations to take legal action or related to the employment relationship, it is necessary to verify the proposed recommendations by the Compliance Officer with legal counsel N and the Director of DHR in terms of their admissibility and in order to determine the next stages of the proceedings.

d) If the investigation concerned violations within the operation of a given organizational unit in N, the preliminary report is forwarded to the Director of N1 managing the audited organizational unit, who has the right to raise any objections to the content of the preliminary version of the report, no later than 3 working days from its receipt. If the Director of N1 managing the audited entity presents reservations regarding the initial version of the report, the Compliance Officer decides whether to include them in the final version of the report. The objections raised are attached to the report on the proceedings in an unchanged form, unless they are included in the content of the report.

e) The investigation report is stored in a dedicated network area that only the compliance officer has access to.

5.2. N1 Director indicated in the recommendation as responsible for implementation is responsible for the implementation of the recommendations and recommendations presented in the report. The timely implementation of recommendations and recommendations is supervised by the Compliance Officer.

5.3. If an explanatory proceeding is conducted on the basis of an order from the Management Board of N, the Supervisory Board of N or its Committees, a report on such proceedings is presented by the Compliance Officer at a meeting of the above-mentioned bodies, respectively, or the Compliance Officer sends the report electronically to the Members of the above-mentioned bodies to the accounts in domain N.

5.4. Materials from the conducted investigations are stored by the Compliance Officer in a dedicated network area to which only the Compliance Officer has access.

5.5. If breaches of the law referred to in the Act are reported, within a maximum of 3 months from the confirmation of the report, the Compliance Officer shall provide feedback to the Whistleblower or, if the confirmation is not provided to the Whistleblower, 3 months from the lapse of 7 days from the date of the report, unless the Whistleblower has not provided a contact address to which the feedback should be provided. Feedback includes, in particular, information on whether or not a violation of the law has been found and any measures that have been or will be taken in response to the identified violation of the law (application of follow-up actions). In the case of other reports, the Compliance Officer sends information to the reporting person about the closure of the investigation and the findings made, if possible.

6. Conducting verification proceedings

6.1. After the deadline for the implementation of all recommendations and recommendations resulting from the report on the explanatory procedure referred to in item 5 above, the Compliance Officer conducts a verification procedure aimed at checking the status of implementation of the recommendations and recommendations.

6.2. If the recommendations or recommendations have not been implemented, the Compliance Officer informs the Management Board of N and N1 Director of the audited organizational unit in N, and then the next steps to implement the recommendations are determined.

6.3. Materials from the verification procedures are stored by the Compliance Officer in a dedicated network area to which only the Compliance Officer has access.

7. Consultation

7.1. A request for consultation on responding to doubts regarding violations of the law, compliance principles and the Code of Ethics can be made through the Compliance Channel.

7.2. Upon receipt of the request, the Compliance Officer evaluates and classifies it.

7.3. In order to respond to the consultation, the Compliance Officer has the right to contact other organizational units in N.

7.4. Answers to consultations are provided only by the Compliance Officer in any form chosen by him/her, as soon as possible.

8. External Submissions

8.1. In the event of a violation of the law referred to in the Act, the Whistleblower may make an external report without first making an internal report. An external report is received by the Commissioner for Human Rights or a public body (supreme and central government administration bodies, local government administration bodies, local government units, other state authorities and other entities performing public administration tasks by virtue of law, competent to take follow-up actions in the areas indicated in Article 3(1) of the Act) and, where applicable, to the institutions, bodies, offices or agencies of the European Union.

Information on possible ways of contacting the above-mentioned authorities can be found on the websites of these authorities.

8.2. An external report made to the Ombudsman or other relevant public authority in disregard of these Rules does not result in the Whistleblower being deprived of the protection provided for in the Act.

9. Final provisions

Section 9.1. The Regulations enter into force after 7 days from the date of their notification to persons performing work in the manner adopted in N.