



NEPI
ROCKCASTLE



WHISTLEBLOWING POLICY

Whistleblowing Policy



1. INTRODUCTION AND PURPOSE

NEPI Rockcastle (the 'Group') is committed to high standards of ethical, moral and legal business conduct. The employees and representatives of the Group must practice honesty and integrity in fulfilling their responsibilities and comply with all applicable laws and regulations.

This Policy is intended to encourage and enable employees and any other external parties to raise serious concerns so that the Group can address and correct inappropriate conduct and actions.

For the purpose of this document, the term "employee/employees" includes all NEPI Rockcastle Group personnel, as well free-lancing collaborators and partners' s personnel performing outsourced activities for or on behalf of Nepi Rockcastle Group entities (e.g. outsourced PM services, property management, development project management), irrespective the nature or the duration of the collaboration/services agreement.

2. APPLICATION

This Policy applies to all companies in the Group and managed joint ventures, as well as to all employees, collaborators, any third party and it aims to:

- encourage employees and external parties to feel confident in raising serious concerns, to question and act upon their concerns;
- provide ways for employees and external parties to raise those concerns;
- reassure employees and external parties that if they raised concerns in good faith and reasonable believe them to be true, they will be protected from retaliation.

3. REPORTING PROCEDURE

The Group has an open-door policy and recommends that employees share their concerns, suggestions or complaints with their supervisor. If an employee is not comfortable with speaking with his supervisor or is not satisfied with the supervisor's response, he is encouraged to send his concerns or complaints, anonymously if he so wants, through a secure web portal hosted on the Group's website in the Corporate Governance section (available to the wide public and any stakeholder), call the Group hotline (the contact number is displayed on the Group website), or provide formal or informal information to Internal Audit / Compliance / Executive Directors.

If an employee has reasonable belief that another employee, a collaborator, a Director or the Group has engaged in any action that violates any applicable law, or regulation, including those concerning accounting and auditing, or which may constitute a fraudulent practice or are in incompliance with the Code of Ethics the employee is expected to immediately report such information on one of the above mentioned channels.

If an external party has reasonable belief that an employee or any member of the Group has engaged in any action that violates any applicable law, or regulation, including those concerning accounting and auditing, or which may constitute a fraudulent practice, he / she may report such information on one of the above-mentioned channels.

All reports received through the official channels will be directed to the Head of Internal Audit, the CEO, the CFO and the Chair of the Audit Committee or to a Board sub-committee that the Board may establish for this purpose. All reports will be reviewed promptly, and, if determined to be necessary, i.e. following a plausibility check, an investigation will be conducted. In conducting its investigations, the Group will strive to keep the identity of the complaining individual confidential (if the complaint was not submitted anonymously), while conducting an adequate review and investigation.

The non-Executive Directors may raise their concerns related to the affairs of the Company to the Audit Committee or using the official Group hotline / the public whistleblowing portal. The Audit Committee may further decide to initiate an investigation, using internal resources (i.e. Internal Audit) or external advisors, as the committee deems appropriate.

4. CONCERNS TO BE RAISED

Employees and others (including external parties) can report in good faith any concerns regarding, but not limited to:

- conduct which is significantly inconsistent with the Group's values, Code of Ethics, standards, procedures, laws, regulations and other legal obligations;
- conduct which is inconsistent with the Group's Accounting Practices, manipulation of accounting records and financial statements;
- conduct which is inconsistent with the Group's Internal Controls as well as gross incompliance with the Group's policies and procedures;
- conduct which is inconsistent with the Group's Health & Safety policies;

- conduct which is materially inconsistent with the environmental, social, governance Group's commitments, including material breaches or actions that may cause harm to the environment, the communities, people in general or Group's employees in particular;
- any allegations of bribery, corruption or conflict of interest;
- theft, misappropriation and embezzlement;
- falsification of documentation and other manipulative action on documents;
- insider trading and market manipulation;
- cyber-crime;
- misuse of private or business secrets;
- money laundering or terrorism financing;
- violation of representation of signature rules.

As regards employees, the purpose of this Policy is not to provide them with a tool to report HR-related issues or grievances specific to the day-to-day operations and job description or human interaction and relationships. Such issues should be directly raised to and solved by the Human Resources Department.

5. NON-RETALIATION

Employees that report matters in good faith will be protected and cannot lose their positions or suffer any form of harassment or occupational detriment as a result. This would equally apply where the whistleblower is mistaken as to the true nature of the issue. Such protection is not afforded to anyone who maliciously raises a matter. The Group guarantees it will not retaliate against an employee because that employee: (a) reports a concern or (b) participates in good faith in any resulting investigation or proceeding. The Group may take disciplinary action (up to and including termination) against an employee who has engaged in retaliatory conduct in violation of this Policy and will take all measures to protect the whistleblower.

External parties filing a complaint under this Policy will not be retaliated against.

Confidentiality will be ensured, to the extent possible, both during the investigation and the reporting process and sensitive information will be disseminated on a 'need to know' basis.

Employees and Directors will be trained on this Policy and the Group's prohibition against retaliation in accordance with this Policy.

6. PRESERVING PRIVACY

In managing the reported cases, under this Policy, the Group applies the following **principles and rules**:

- implement dedicated channels for internal and external reporting and specific rules where the purpose is clearly specified;
- preserve confidentiality of the information received and protect the whistleblowers' identity and all other persons involved;
- apply data minimisation principle (only process personal information, which is adequate, relevant and necessary, for the particular case);
- ensure, when responding to right of access requests, that personal information of other parties is not revealed;
- limit the transfer of personal information only when necessary for the legitimate performance of tasks covered by the competence of the recipient;
- set the storage periods for the personal information processed within the scope of this Policy, depending on the outcome of each case;
- implement organisational and technical security measures in order to guarantee a lawful and secure processing of personal information.

Personal data. Under this Policy, Personal information means any information that relates to an identified or identifiable natural person, as defined by data privacy legislation, including an individual's activities, such as his or her working relations and economic or social behaviour.

Data minimisation

- The Group recommends whistleblowers to refrain from providing in their statements, details regarding the health state of another person or other details regarding sensitive data belonging to another person (e.g. religious, political or sexual orientation etc.); where in her/his statement, the whistleblower happens to disclose such information, The Group will not process it and will either delete or return it to the sender.
- When access is granted to the personal information of any concerned individual, the personal information of third parties such as informants, whistleblowers or witnesses should be removed from the documents except in exceptional circumstances, if (i) the whistleblower authorises such a disclosure, (ii) this is required by any subsequent criminal law proceedings or (iii) the whistleblower maliciously makes a false statement.

Access to reports. Access to the whistleblowing report and involved parties shall be granted to a limited number of persons, authorised internally to run the

investigation (generally part of Internal Audit, Legal, Compliance). Also, subject to the evolution of the investigation, the personal data might be disclosed to competent judicial authorities.

Outsourcing. To ensure efficient handling, as well transparent and objective investigation of the Whistleblowing cases, the Group may decide to contract specialised external providers, in which case (i) adequate data processing arrangements/clauses are to be signed, as well (ii) transparent information thereof is to be provided to the whistleblowers by the means of the **Whistleblowing Data Privacy Policy** (document published on the Group's website).

Storage.

- Personal information shall not be kept for a longer period than necessary having regard to the purpose of the processing, while personal information that is not relevant to the investigations shall not be further processed.
- When an initial assessment is carried out but it reveals that the case is not within the scope of this Policy, then the report shall be deleted or referred to the right channel.
- In case of closed cases, references thereto and relevant documentation shall be kept for audit purposes or in case they are needed in litigations or other similar procedures, for a period of 10 (ten) years.

Information and transparency. The coordinates of the processing of whistleblowers' personal data by the Group, as Data Controller, are detailed in the **Whistleblowing Data Privacy Policy**, published on the Group's website.

7. INVESTIGATION PROCEDURE

Following the plausibility check performed by Internal Audit, all reported incidents considered plausible will be investigated. All reports will be dealt with in confidence, with only staff that need to know, being informed. The hierarchical supervisor of the concerned employee (s) does not need to be informed, unless the investigation team considers such information may bring additional value in the investigation process.

Where the individuals raising the concern have identified themselves, they may be approached during the investigation, in a confidential manner, in order to provide additional information and support with the investigation process. The Group encourages the potential whistleblowers to disclose their identity and

therefore be able to provide additional information, if needed. If the individuals specify during such interaction or include in their tip off that they would like to be kept up to date with the progress of the investigation, they will receive subsequent information, unless such disclosure may jeopardize the investigation result or hinder confidentiality.

Internal Audit will be responsible to perform the investigation, in accordance with the principles and quality requirements laid down in the Internal Audit Charter and may collaborate in doing so with subject matter experts from Risk & Compliance, Legal or other functions as it considers necessary.

Once the facts have been established, corroborated and documents reviewed by the investigation team, the individual(s) potentially implicated may be informed of the tip off so long as doing so does not jeopardise the investigation outcome and confidentiality and whistleblower protection principles are followed strictly. The information provided to the individual may include:

- Who is responsible for investigating the allegation;
- The object of accusations;
- Who will receive the investigation report;
- How the individual can exercise their rights of access, rectification and erasure of any misinformation in relation to personal data.

If individuals are not satisfied with the response received and any subsequent action taken, they may put their concerns in writing to the Chair of the Audit Committee who will arrange any further investigation as he thinks appropriate. The Chair of the Audit Committee has the ability to seek external advice if this is merited. The Chair of the Audit Committee will also provide a response to the individual concerned.

The results of the investigation, together with any recommended measures, including consequence management, will be reported to the Audit Committee on a regular basis by the Head of Internal Audit.

This Policy is reviewed and updated at least on an annual basis, published internally on the Group's internal network and on its website. The review will be performed by a team of Legal, HR, Data Privacy, Internal Audit and Compliance professionals, in order to ensure it is comprehensive and up to date. The Policy is approved by the Board of Directors and published on the Group's website, to be accessible to all parties concerned.

Approved by the Board of Directors of NEPI Rockcastle N.V.

