



Speak Up: Raising Concerns and Non-Retaliation Policy

Policy Owner: Chief Internal Audit and Compliance Officer
Effective Date: December 1 2022

I. Delegation and GRC Framework

This Speak Up: Raising Concerns and Non-Retaliation Policy (the “Policy”) is part of the GRC Framework. Any questions of interpretation or conflict should be referred, in the first instance, to your supervisor, relevant department head or the relevant OpCo Policy owner and, in the second instance, to the Group Policy owner.

II. Purpose, applicability and scope

One of VEON’s core values is truthfulness, and implicit in this value is the need for transparency and openness across the VEON Group. Anyone who has information on Breaches should promptly Report using the channels described in this Policy.

This Policy applies to the VEON Group, VEON Group Personnel, Business Partners, as well as Reporters. In accordance with the VEON Joint Venture Governance Policy, controlled entities and joint ventures will adopt this Policy, and the VEON Group will use best efforts to ensure compliance with this Policy in non-controlled joint ventures (i.e., entities in which VEON or a member of the VEON Group owns a 50% stake or less).

This Policy sets the minimum standards and requirements that must be followed. Local laws, regulations, or rules that impose higher standards and requirements will prevail and must be adopted in local policies and procedures. A VEON Group entity may adopt stricter standards than those set forth in this Policy.

However, an OpCo must obtain written approval from the Policy Owner (following consultation with Group Legal) before adopting any less strict standard set forth in this Policy.

III. Definitions

Capitalized terms within this Policy shall have the meanings set forth in Appendix A.

IV. Minimum requirements and standards

Speak Up: Raising Concerns and Non-Retaliation Policy	
Summary:	This Policy establishes standards of conduct and practice for Reporting potential or known Breaches or attempts to conceal potential or known Breaches. It is not intended to apply to general customer complaints (e.g., service quality, pricing) or individual employment concerns (e.g., regarding bonuses, performance reviews, managerial decision-making, etc.) that do not qualify as Breaches. Customer complaints are handled by the customer service function, and individual employment issues should be reported to the

	employee's line manager or Human Resources.
Objectives	<p>The objectives of this Policy are:</p> <ul style="list-style-type: none"> - to make clear that knowledge of potential or known Breaches involving or implicating VEON, VEON Group companies, VEON Group Personnel or Business partners must be promptly reported; - to provide information on how to properly report Breaches; - to ensure that Reporters are able to report Breaches without fear of retaliation.
Risks	<p>a) Risks of Breach of Confidentiality and Anonymity of Reports: Reports which are subject to investigation are often sensitive and, at times, present the potential of liability to the VEON Group and/or OpCos, and/or individuals. VEON handles Reports confidentially and according to applicable laws and regulations. Whichever method of Reporting is selected, when anonymity is requested, VEON will work to preserve anonymity as permitted under local law.</p> <p>b) Risk of Retaliation: Reporters should feel comfortable Reporting Information on Breaches. VEON will not tolerate any type of Retaliation including threats of Retaliation and attempts of Retaliation against any Reporter who in good faith Reports Information on Breaches.</p>
Controls	<p>VEON undertakes to ensure, when required by applicable law, that:</p> <ul style="list-style-type: none"> a) channels for receiving the Reports are designed, established and operated in a secure manner that ensures protection of the confidentiality of the identity of the Reporter and of any third party mentioned in the Report, and prevents access thereto by non-authorised staff members; b) an acknowledgment of receipt of the Report is sent to the Reporter within seven (7) calendar days of that receipt; c) an impartial person or department competent for Following-up on the Reports is designated, which may be the same person or department as the one that receives the Reports and which will maintain communication with the Reporter and, where necessary, ask for further information from and provide feedback to that Reporter; d) the designated person or department referred to in point (c) above diligently Follows-up, including as regards anonymous Reporting pursuant to the applicable laws;

	<p>e) feedback is provided within a reasonable timeframe not exceeding three (3) months from the acknowledgment of receipt of the Report.</p>
<p>Minimum requirements and standards</p>	<p>Ensuring transparency and openness and promoting Reporting is fundamental; in turn, the making of a Report must be done with honesty and integrity and on an informed basis. Knowingly making a false Report, or making a Report in bad faith, is contrary to VEON’s Code of Conduct (the “Code”) and will be considered a violation of this Policy.</p> <p>In deciding what Reports should be investigated by Group Investigations or OpCo Investigations, Group Investigations and OpCo Investigations will consider materiality, significance, and risk for VEON Group or for the relevant OpCo.</p> <p>Reporting Information on Breaches does not allow an employee to neglect his/her job duties, violate employer rules, or do anything else that would otherwise result in poor performance or misconduct. VEON has the right to discipline or even terminate employees for poor performance or improper behavior, even if the employee made a honest Report about a possible Breach.</p> <p>Reporters should feel comfortable Reporting Information on Breaches. VEON will not tolerate any type of Retaliation including threats of Retaliation and attempts of Retaliation against any Reporter who in good faith Reports Information on Breaches.</p> <p>Examples of forms of Retaliation are: (a) suspension, lay-off, dismissal or equivalent measures; (b) demotion or withholding of promotion; (c) transfer of duties, change of location of place of work, reduction in wages, change in working hours; (d) withholding of training; (e) a negative performance assessment or employment reference; (f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty; (g) coercion, intimidation, harassment or ostracism; (h) discrimination, disadvantageous or unfair treatment; (i) failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment; (j) failure to renew, or early termination of, a temporary employment contract; (k) harm, including to the person's reputation, particularly in 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) cancellation of a license or permit; (o) psychiatric or medical referrals.</p> <p>Any VEON employee who takes adverse actions that can be regarded as Retaliation against others for making a Report in good faith, or otherwise Retaliates or attempts to Retaliate, will be subject to disciplinary action. An employee who believes they have experienced Retaliation for Reporting Information on Breaches, should immediately inform VEON Compliance, Investigations, Legal, or Human Resources.</p>

VEON encourages Reporters to provide as much information as possible when making a Report. Providing detailed information will help VEON determine the best way to address the Report. Failure to provide all relevant information may inhibit VEON's ability to conduct a thorough and swift Follow-up.

When making a Report, it is helpful to provide:

- The name, title, and/or department of the person who engaged in the Breach that is the subject of the Report;
- The date when the Breach occurred (month, year, and date, if known);
- Whether anyone has previously raised this Breach to anyone else at VEON and what (if any) actions occurred after the Report was raised;
- Whether the Reporter would like to remain anonymous; and
- Contact information, so that VEON may follow up with the Reporter as appropriate. Without contact information, VEON will not be able to contact the Reporter once a Report has been made.

Reports of Information on Breaches under this Policy may be raised through any of several channels, at the choosing of the Reporter. Certain channels allow for anonymity as indicated below.

Reporting Method	Channels
Direct Reports	VEON Group Personnel may make direct Reports to: <ul style="list-style-type: none"> - A line manager; - Another manager or supervisor; - Representatives of the Compliance, Investigations, Legal, or Human Resources departments.
E-mail Group SpeakUp Channel	Individuals may Report Information on Breaches or ask questions to Group Investigations at compliance@veon.com
Online	VEON maintains a confidential case management system that is available worldwide to Report Information on Breaches, accessible at https://www.veon.com/speakup When making a Report online, individuals will have the option to request anonymity (i.e., to not disclose the Reporter's name or contact information), in which case the Reporter should be aware that no Feedback is possible.
By phone/hotline	Individuals may Report Information on Breaches by telephone. Telephone numbers are available

		<p>on the https://www.veon.com/speakup webpage</p> <p>The call will be answered by a third-party operator, and the Report will be entered into the case management system for review by VEON.</p> <p>When making a Report by phone, individuals will have the option to request anonymity (i.e., to not disclose the Reporter’s name or contact information), in which case the Reporter should be aware that no Feedback is possible.</p>
	<p>External Reporting</p>	<p>Any Reporter that is an employee (or ex-employee, self-employed, volunteer or intern) based in the Netherlands who suspects a possible wrongdoing within VEON Group subsidiary registered in the Netherlands can get confidential advice from the Dutch Whistleblowers Authority, free of charge. The wrongdoing has to involve a public interest and must be based on reasonable suspicion as well. If these conditions meet the Reporter’s personal situation, such Reporter can contact the Dutch Whistleblowers Authority via: advies@huisvoorklokkenuiders.nl</p>

V. Assurance

- VEON takes all Reports of Breaches seriously and is committed to Follow-up on all credible allegations. Anyone who receives a Report covered by this Policy must treat the Information on Breaches as confidential and with discretion, as well as treat the Reporter and the subject of the Report with respect and maintain their anonymity if so requested by the Reporter. The person who received the Report should either enter it into VEON’s Case Management System (CMS) using the website (<https://www.veon.com/speakup>), submit a message to Compliance@veon.com , or report it to Group or Local Ethics & Compliance or Investigations.
- Group Investigations periodically reviews the status of the investigations conducted by OpCos based on Reports received (case aging, completeness of documents prepared for each investigation, correctness of selected Tier of OpCo conducted investigations, status of the remediation measures and disciplinary actions recommended as a result of each investigation, etc.).
- If a Report credibly alleges wrongdoing by a member of Group or Opco Investigations, Ethics & Compliance, Legal, Human Resources, Security or another function that conducts investigations, consideration must be given to assigning the matter to an Investigator outside that function, to avoid any perception that the investigation lacks objectivity.

- External Auditors may conduct periodic audits of the investigations conducted based on Reports.
- Management self-assessment -> management certification.

VI. Management certification

As part of the VEON Management Certification process, certain representations will be required from VEON Group Entity Management and select members of key management at VEON HQ. Representations with respect to compliance with the requirements of this policy will be included in the Management Certification as deemed necessary by the Policy Owner.

VII. Where to go for help?

If you have questions about this Policy, please contact, in the first instance, your supervisor, the relevant department head or the relevant OpCo Policy owner and, in the second instance, the Group Policy owner.

If you believe that someone may have violated this Policy or any other VEON policy or procedure, please contact your Local Ethics & Compliance Officer or Group Compliance at compliance@veon.com, or submit a report about the violation at www.veon.com/speakup. VEON does not tolerate any form of retaliation, harassment, or intimidation of any person who reported an alleged violation in good faith.

VEON will investigate the alleged misconduct in relation to this Policy or any other VEON policy and procedure in accordance with the VEON Investigations Management Policy and the Investigations Procedure. Any member of the VEON Group Personnel who violates this Policy may be subject to disciplinary measures, up to and including termination of employment.

VIII. Reference Documents

The following related documents provide additional rules, guidance and procedures:

- VEON Code of Conduct
- Joint Venture Governance Policy
- VEON Investigations Management Policy
- VEON Investigations Procedure

This Policy and other policies, procedures and guidelines can be found in the House of Policies on the VEON Group intranet.

IX. Document History

Effective Date	Revision	Reason/Description
December 1 2022		Initial Release.

APPENDIX A: Definitions

Business Partner	Any counterparty of VEON Group as defined by Third Party Risk Management Policy
Breaches	Any acts or omissions that (1) are unlawful under the applicable laws or regulations, (2) defeat the object or the purpose of the applicable laws or regulations, and/or (3) are violations of VEON Group or OpCo policies and procedures.
External Reporting	Oral or written communication of Information on Breaches to the competent authorities.
Feedback	The provision to the Reporter of information on the action envisaged or taken as Follow-up and on the grounds for such Follow-up.
Follow-up	Any action taken by the recipient of a Report to assess the accuracy of the allegations made in the Report and, where relevant, to address the Breach reported, including through actions such as an internal enquiry, an investigation, an audit, an action for recovery of funds, or other relevant actions.
Information on Breaches	Information, including reasonable suspicions, about actual or potential Breaches, which occurred or are very likely to occur in VEON Group or in another organization with which the Reporter is or was in contact through his or her work for VEON Group, and about attempts to conceal such Breaches.
Report	Any concerns or allegations of possible violations of VEON's Code of Conduct, policies, procedures or the law, raised through any of several channels indicated in section Error! Reference source not found. herein, such as: <ul style="list-style-type: none"> • In-person, e-mail or postal letter reports; • VEON's independently operated web/phone intake system: https://www.veon.com/speakup; • E-mails to VEON's Group Ethics & Compliance e-mail address (compliance@veon.com); or • E-mails to OpCos' compliance e-mail addresses (where applicable).
Reporter	Any person who makes a Report.
Retaliation	Any direct or indirect act or omission that occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and, which causes or may cause unjustified detriment to the Reporter.
VEON Group	VEON Ltd. (VEON) and any company (OpCo) that is directly or indirectly wholly or majority-owned or otherwise controlled by it. Note that the requirements for non-controlled entities (i.e., entities in which VEON or members of the VEON Group own a 50% stake or less) are set out in the VEON Joint Venture Governance Policy.
VEON Group Personnel	Any director, officer, or employee of VEON or a member of the VEON Group.