Information on the Whistleblower Policy (2026)

Purpose and Scope

The whistleblower channel of the Bank may help to discover (potential) breaches that have (or could have) serious adverse consequences for the financial standing, performance and/or reputation of Nexent Bank or a Nexent Bank group company.

There may be occasions when a Reporting Person has information on (potential) breaches. The purpose of the whistleblower channel is to ensure that there is a process whereby information on (potential) breaches can be escalated swiftly for investigation and resolution, in confidence and without fear of retaliation against the Reporting Person or against facilitators, third persons (e.g. coworkers or relatives) or legal entities connected to the Reporting Person. Nevertheless, in normal circumstances the basic principle is that a Reporting Person must initially express any information on (potential) breaches to his/her manager.

Breaches are acts or omissions that are unlawful, unethical or otherwise qualify as misconduct, or defeat the object or purpose of the internal and external rules and regulations applicable to Nexent Bank, for example in relation to:

- The integrity of Nexent Bank's channels (i.e., to help ensure that channels work as intended).
- Accuracy and completeness of information (financial reporting and management information).
- Ethical standards, such as those laid down in Nexent Bank's Code of Conduct.
- Rules aimed at risk avoidance or risk limitation.

Who can report?

The whistleblower channel can be used by Reporting Persons, meaning:

- Workers: This includes employees, persons with a contract of employment/employment relationship with a temporary agency and other non-standard employment relationships.
- Self-employed persons: This includes suppliers and consultants providing goods or services to Nexent Bank, freelance workers and (sub)contractors;
- Shareholders and persons belonging to the management and supervisory body to the extent that they do not qualify as Worker, as well as volunteers and paid or unpaid trainees;
- Any persons working under the supervision and direction of (sub)contractors and suppliers.

How to report?

Prior to using the whistleblower channel, the basic principle is that the Reporting Person is encouraged - but not obliged - to report any suspected (potential) breach initially to:

- his/her immediate manager or, if that is inappropriate,
- the next level of line management, or if such reporting would be inappropriate, the level afterwards and so on, up to the level of the Chair of the Supervisory Board.

Prior to the reporting of a suspected (potential) breach, a Reporting Person may wish to obtain internal or external advice. In case the Reporting Person wish to receive an internal advice, the Reporting Person can approach the Group Head of Compliance in Head Office. In the event the internal advice given by Group Head of Compliance results in the reporting of a (potential) breach, Group Head of Compliance will be excluded from any participation in further inquiries concerning the contents and/or merits of the submitted report.

The Reporting Person can resort to the whistleblower channel if he/she feels his/her concerns have not been properly addressed, if line management is part of the problem, or if there is some other reasonable objection or practical obstacle to using the primary channel as described hereinabove. In such cases, the Reporting Person may raise his/her information on (potential) breaches with Compliance in the respective Nexent Bank, location or, if the Reporting Person prefers not to discuss the matter with that unit, with Compliance in Head Office.

Anonymous reporting

In lieu of the whistleblower channel and the use of the corresponding whistleblower channel form in full, a Reporting Person may prefer to file an anonymous report.

However, Reporting Persons who choose to report anonymously must note that anonymous reporting has certain drawbacks. The ability to investigate, carry out follow-ups and provide feedback is reduced.

It will also be more difficult to ensure that the Reporting Person is protected if their identity is not known.

In certain jurisdictions, including the Netherlands, Germany and Malta, Reporting Persons reporting information on (potential) breaches anonymously do not fall within the scope of regulations protecting whistleblowers, unless they are subsequently identified and/or suffer retaliation. Nexent Bank therefore strongly encourages Reporting Persons to disclose their identity or at least provide contact details to facilitate follow-ups.

Confidentiality

Compliance and others involved in looking into the Reporting Person's information on (potential) breaches will make every effort to maintain confidentiality of the report and of the person filing the report, if known. They will not disclose the Reporting Person's identity, if known, to anyone directly involved in the case in question without the Reporting Person's prior consent.

In the event there are compelling reasons for Nexent Bank to report the (potential) breach to external authorities and thus be obliged disclose information that would otherwise be kept confidential, the Reporting Person will be informed, to the extent possible, and Nexent Bank will provide the necessary support.

Protection against retaliation

The reporting of any information on (potential) breaches in good faith or participation in a related investigation will never result in termination of employment or any other improper deviation from the employment contract of the person reporting information on (potential) breaches. Reporting Persons are protected against these and other forms of retaliation.

Persons assisting a Reporting Person in the reporting process in a work-related context (i.e., facilitators), coworkers and/or relatives of the Reporting Person and legal persons that the Reporting Person owns, works for or is otherwise connected with, are also protected against retaliation.

Involvement in malpractice

It may happen that a Reporting Person wishes to report a malpractice in which he/she has been a party. In such cases, the Reporting Person must answer for his/her own actions and will not be immune from disciplinary or criminal proceedings, although the fact that he/she has brought the information on (potential) breaches to light will be considered.

Malicious actions

Deliberately reporting information on (potential) breaches known to be incorrect or misleading at the time of reporting may, depending on the circumstances of the case, qualify as malicious, frivolous and/or abusive. In such cases, the Reporting Person will not be protected by this Policy. At the same time, protection is not lost where the Reporting Person reported inaccurate information on (potential) breaches by honest mistake.

If it appears after investigation that the Reporting Person acted out of malice when he/she raised the information on (potential) breaches, the matter will in all cases be referred to the Human Resources function in the respective Nexent Bank location. In such an event the Human Resources function involved will consider whether the management responsible for the Reporting Person must be advised to take disciplinary action towards the Reporting Person. In addition, the Reporting Person may face legal consequences in this respect.

Following up after reporting

If Compliance considers prima facie that the report meets the criteria of the whistleblower channel, they will confirm receipt of the report to the Reporting Person within 7 (seven) days if the identity of the Reporting Person who filed the report is known to Compliance.

If Compliance considers the criteria for application of the whistleblower channel have not been met or if they think that there is a more appropriate procedure, and if the identity of the Reporting Person who filed the report is known to Compliance, they will inform the Reporting Person accordingly within 7 (seven) days of receiving the report.

If Compliance accepts the report, they will then consider whether further inquiries are necessary, and if so, will initiate those inquiries. They may request the assistance of other functions, such as Information Security Management, Legal and Internal Audit, or external parties.

If the Reporting Person of a branch or liaison office notifies his/her information on (potential) breaches to Compliance in Head Office, they, with due respect for the confidential nature of the information, will consult their local respective Compliance counterpart on the matter, unless the Reporting Person has sound objections to such consultation.

Compliance will provide the Reporting Person with feedback within three months from the acknowledgement of receipt of the information on (potential) breaches. The feedback will include information on the action(s) envisaged or taken as follow-up and the grounds for such follow-up. A follow-up could mean any action taken by Nexent Bank 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, prosecution, an action for recovery of funds. It could also be the closure of the procedure.

Reporting Persons who report their concerns about (potential) breaches within Nexent Bank or within a Nexent Bank group company must keep full confidentiality about their filing of the report, the details of their report, the possible feedback they have received and, in all events, not disclose any information other than in a manner as and if described within this Policy and with the explicit consent of Compliance.

External whistleblower channels

The Netherlands

In the Netherlands, a Reporting Person may have the option to report information on (potential) breaches directly to either the so-called House of Whistleblowers or to the Dutch Central Bank.

The House for Whistleblowers will commence an investigation when the (potential) breach is sufficiently serious and well-founded.

Similarly, the Dutch Central Bank will commence an investigation if a Reporting Person would not have been able to easily notify a (potential) breach internally and only if such (potential) breach details a grave breach of (financial law) legislation.

Information on (potential) breaches of specific regulations may be reported by using other external reporting channels.

For example, (potential) breaches of the Market Abuse Regulation can be reported externally to the Authority for the Financial Markets

(Potential) breaches of the General Data Protection Regulation can be reported to the Data Protection Authority.

Germany

In Germany, a Reporting Person may notify a (potential) breach directly to the regulator, i.e., Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

Malta

In Malta, a Reporting Person may notify a (potential) breach directly to Malta Financial Services Authority (MFSA), For this, a special Whistleblowing External Disclosure Form has been designed by MFSA and published on their website.

Romania

In Romania, a Reporting Person may notify a (potential) breach directly to the National Bank of Romania (NBR) and the National Integrity Agency (ANI), the authority designated to handle reports received in its capacity as an external reporting channel. More information can be found on the website of respectively both institutions.

Also, information on (potential) breaches of specific regulations may be reported directly to the competent authority in that field. For example, (potential) breaches of the consumer protection requirements can be reported directly to the National Authority for Consumer Protection (NACP). (Potential) breaches of the General Data Protection Regulation can be reported to the National Supervisory Authority for Personal Data Processing (NSAPDP).

***