Information on the Internal Alert System (Whistleblower System)

The Internal Alert System ("IAS"), also referred to as the whistleblower system, of Nexent Bank N.V. (hereinafter "Nexent 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 IAS 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, under normal circumstances, the basic principle is that a Reporting Person must initially express any information on (potential) breaches to their manager.

Purpose and scope of the Internal Alert System

The IAS is meant to cover (potential) breaches. 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 systems (i.e., to help ensure that systems 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 use the Internal Alert System?

The system 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 of Nexent Bank 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 use the Internal Alert System?

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

- their 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 Nexent Bank's 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 wishes to receive an internal advice, the Reporting Person can approach Group Head of Compliance in Nexent Bank's 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 IAS if they feel their 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 may report information on (potential) breaches to Compliance at the relevant Nexent Bank location or, if preferred, directly to Compliance at Nexent Bank's Head Office.

Reporting Persons are strongly advised to use the designated IAS Notification Form, when raising information on (potential) breaches. This will help both the Reporting Person and the recipient to assess whether the matter falls within the framework of the IAS and will foster an expeditious handling of the matter.

The IAS Notification Form is published on the designated Internal Alert System (Whistleblower) section on Nexent Bank's intranet page as well as under the Compliance section in PolicyHub. Reporting

Persons who do not have access to these sections can find the IAS Notification Form on Nexent Bank's corporate website (downloads section).

Anonymous reporting

In lieu of the IAS and the use of the corresponding IAS Notification 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.

However, it cannot be guaranteed that third parties will not find out the Reporting Person's identity by other means. In the event there are compelling reasons for Nexent Bank to report the (potential) breach to external authorities, the Reporting Person will be informed, to the extent possible and allowed, and Nexent Bank will give such Person all 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 they have been a party. In such cases, the Reporting Person must answer for their own actions and will not be immune from disciplinary or criminal proceedings. However, their decision to report the (potential) breach will be taken into consideration as a mitigating factor.

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 Nexent Bank's whistleblower system. 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 they 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 IAS, 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 IAS 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.

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.

If the investigation concludes that there has been no (potential) breach or if there is insufficient evidence of this, Compliance will inform the Reporting Person accordingly if the identity of the Reporting Person who filed the report is known to Compliance.

External whistleblowing procedures

The Netherlands: In the Netherlands, a Reporting Person may have the option to report information on (potential) breaches directly to the so-called House of Whistleblowers (*Huis voor Klokkenluiders*), to the Dutch Central Bank (DNB) or to the Authority for the Financial Markets (AFM).

Germany: In Germany, a Reporting Person may notify a (potential) breach directly to the regulator, i.e., Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). For this, BaFin has implemented a Whistleblowing Platform

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), For this, a special Whistleblowing External Disclosure Form has been designed by NBR and published on their website.

Amsterdam, June 2025