Internal Alert System
(*Whistleblower*) *Policy*

Credit EuropeBank

Amsterdam, August 2023

Credit EuropeBank

Internal Alert System
(*Whistleblower*)
Policy

Effective Date	August 2023
Approval Authority	Managing Board
Owner	Compliance
Contact Function	Compliance
Classification	CEB Internal
Functional Applicability	Credit Europe Bank N.V.
Geographic Applicability	NL, DE, MT, TR
Initial Creation Date	3 October 2008
Last Reviewed	August 2023
Next Review Date	August 2025
Version	2.6
Status	Approved

Table of Contents

1. Introduction

The Internal Alert System of Credit Europe Bank N.V., i.e. Head Office, branches and overseas liaison office (hereinafter "CEB"), also referred to as the Whistleblower System, may help to discover (potential) breaches that have (or could have) serious adverse consequences for the financial standing, performance and/or reputation of CEB or a CEB group company.

There may be occasions when a Reporting Person has information on (potential) breaches. The purpose of the Internal Alert System 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.

The Managing Board of CEB is responsible for the implementation of the Internal Alert System and the Compliance Division (hereinafter referred to as "Compliance") has been given the task of maintaining the system.

2. What is the purpose of the Internal Alert System?

2.1 Scope

The Internal Alert System 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 CEB, for example in relation to:

- The integrity of CEB 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 CEB's Code of Conduct.
- Rules aimed at risk avoidance or risk limitation.

If this Policy would conflict with any applicable local law and/or regulation, the local law and/or regulation prevails.

2.2 Definitions

Information on (potential) breaches
Information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in CEB, and about attempts to conceal such breaches. Such information must be acquired in a work-related context. Information which is already fully available in the public domain is not in scope of this Internal Alert System (Whistleblower) Policy (hereinafter "Policy");

Reasonable grounds for suspicion
Reporting Persons must have reasonable grounds to believe, in light of the circumstances and the information available to them at the time of reporting, that the matters reported by them are true and constitute a (potential) breach; hard evidence is not required. It is certainly not intended that the Reporting Person him/herself must make inquiries into the facts of the matter. However, only unsubstantiated rumours and hearsay will not suffice as reasonable grounds for suspicion.

Reporting Person
A natural person that falls within the scope as described in chapter 3 of this Policy and discloses information on (potential) breaches acquired in the context of his or her work-related activities.

Retaliation
Any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting, and which causes or may cause unjustified detriment to the Reporting Person.

Work-related context
Current or past work activities at CEB through which, irrespective of the nature of those activities, information on (potential) breaches is acquired. The Internal Alert System is not meant to deal with issues related to the performance of a Reporting Person's employment contract nor to (inter)personal grievances. Normal Human Resources procedures will apply in such cases. Moreover, specific procedures, such as local procedures for reporting harassment (including sexual harassment), must be followed before making use of CEB's Internal Alert System. Even though the use of the Internal Alert System is encouraged in the proper circumstances, its use is optional, not compulsory.

3. 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 CEB, 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**.

This Policy also applies to:

- Reporting Persons whose work-based relationship is yet to begin in cases where information on (potential) breaches has been acquired during the recruitment process or other pre-contractual negotiations; and
- Reporting Persons where they report information on (potential) breaches acquired in a work-based relationship which has since ended.

4. How to use the Internal Alert System?

Prior to using the Internal Alert System[1], 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 Group Head of Compliance in CEB 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 Internal Alert System 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 CEB location or, if the Reporting Person prefers not to discuss the matter with that unit, with Compliance in CEB Head Office.

[1] In Germany, a third-party acts as internal channel, also referred to as Ombudsman, and is therefore to be considered as Internal Alert System.

Reporting Persons are strongly advised to use the designated Internal Alert System form, also referred to as 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 Internal Alert System and will foster an expeditious handling of the matter.

The IAS Notification Form is published on the designated Internal Alert System (Whistleblower) section on CEB's intranet page as well as under the Compliance section in CEB Rules. Reporting Persons who don't have access to these sections can find the IAS Notification Form on CEB's corporate website (downloads section).

While preference is given to the IAS Notification Form, Reporting Persons may report information on (potential) breaches through other means, such as:

- by other written means;
- verbally, via telephone or through other voice messaging systems; and
- by physical meeting, if at the explicit request of the Reporting Person.

5. Anonymous Reporting

In lieu of the Internal Alert System and the use of the corresponding IAS Notification Form in full, a Reporting Person may prefer to file an anonymous report.
Anonymous reporting is a possibility within CEB, as CEB would rather receive anonymous reports than not having information on (potential) breaches reported at all.

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. CEB therefore strongly encourages Reporting Persons to disclose their identity or at least provide contact details to facilitate follow-ups. Confidentiality will always be maintained in accordance with chapter 6 below.

The above means that CEB will investigate anonymous reporting of information on (potential) breaches, but the provisions set out in this Policy (except for confidentiality) and any affiliated documents will not apply to the Reporting Person reporting anonymously until such time as the identity of the Reporting Person becomes known, unless required otherwise by law.

Anonymous reports can be filed in any way which a Reporting Person may prefer. However, the more information that can be disclosed, the better the chances are the report will (be able to) serve as the foundation for further investigation. To that end, it is recommended to make use of the IAS Notification Form whereby information is to be disclosed to the extent the Reporting Person filing the report is comfortable with. To ensure full anonymity, a report can be sent to Compliance by internal mail in a blank envelope.

6. 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, the Internal Alert System cannot guarantee that third parties will not find out the Reporting Person's identity by other means. In the event there are compelling reasons for CEB to report the (potential) breach to external authorities, the Reporting Person will be informed, to the extent possible and allowed, and CEB will give him/her all necessary support.

7. 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.

8. Reporting Person's 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 taken into account.

9. 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 CEB 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.

10. Submitting reports and dealing with information on (potential) breaches

If Compliance considers prima facie that the report meets the criteria of the Internal Alert System, 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 Internal Alert System 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 CEB 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 in a CEB location will inform Compliance in CEB Head Office about the cases they handle under the Internal Alert System.

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 CEB 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.

If, on the contrary, investigation concludes that there are sufficient grounds to assume a (potential) breach, Compliance will notify the appropriate management accordingly, and advise on any further action(s)[2]. Ultimately, it is for management to decide whether the situation justifies action and, if so, what type of action. If the respective management is the subject of the report, it will then be discussed with the next higher level of (line) management. The responsible management will inform Compliance of any decision. Compliance will then inform the Reporting Person of that decision, if such information provision is deemed appropriate.

[2] Such action may include the advice to report the information on (potential) breaches to the Supervisory Board of CEB or competent authorities, where appropriate.

In a situation where a submitted report involves a Managing Board member and there are sufficient grounds to assume a (potential) breach, Compliance in CEB Head Office will notify the Chair of the Supervisory Board who will decide whether the situation justifies action and, if so, what type of action.

The Chair of the Supervisory Board will inform Compliance of any decision and he/she will discuss with Compliance the details of the decision to be disclosed to the Reporting Person if the identity of the Reporting Person who filed the report is known to Compliance.

11. Post-Disclosure Issues

The Reporting Person will receive general information on the report (and its outcome) unless:

- the Reporting Person filed the report anonymously;
- the Reporting Person prefers not to be informed;
- this would be detrimental to the Reporting Person;
- a regulatory requirement or instruction from a competent authority (temporarily or permanently) prevents disclosure to the Reporting Person; or
- there are other valid reasons not to inform the Reporting Person.

CEB can in general not share information with regard to (i) any disciplinary action against a Reporting Person and (ii) any investigation by a regulator or law enforcement agency which is considered confidential itself.

Reporting Persons who report their concerns about (potential) breaches within CEB or within a CEB 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.

12. External Whistleblowing Procedures[3]

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 (*www.huisvoorklokkenluiders.nl*) or to the Dutch Central Bank (*https://www.dnb.nl/en/contact/reporting-complaints-and-wrongdoing/reporting-integrity-incidents-at-financial-institutions/form-dnb-integrity-reporting-desk/*).

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 (*https://www.afm.nl/nl-nl/contact/meldpunt-financiele-markten*). (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) (*http://www.bafin.de*). For this, BaFin has implemented a Whistleblowing Platform (*https://www.bafin.de/DE/DieBaFin/Hinweisgeberstelle/hinweisgeberstelle_node.html*).

Malta

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

General

Regardless of the possibility of external whistleblowing as mentioned above, Reporting Persons are strongly encouraged to work with Compliance rather than directly approaching a supervisor or other competent authorities.

[3] Authorities may from time to time change the URL address of the respective webpage. Therefore, if the page cannot be reached, please visit the regulator's official website.

13. Reporting to Non-Financial Risk Committee

Compliance maintains an internal register with all reported (potential) breaches under this Policy.

Group Head of Compliance or his replacement if he/she is absent has to present quarterly to the Non-Financial Risk Committee a summary of the reports received through the Internal Alert System. Under no circumstances, the identity of any Reporting Person who filed a report may be disclosed during such meetings.

14. Reporting to the Compliance Oversight Committee

Group Head of Compliance or his replacement if he/she is absent has to present to the Compliance Oversight Committee in their regular meetings an overview of incidents which have been reported through the Internal Alert System. Under no circumstances, the identity of any Reporting Person who filed a report may be disclosed during such meetings.

15. Record Keeping

All information, correspondence and documentation relating to a report filed through the Internal Alert System are kept with Compliance[4] in accordance with confidentiality requirements set out in this Policy for at least six years from the date on which the investigation of a report has ended.

All IAS Notification Forms and affiliated documents are stored in a secure manner and are only accessible to authorized personnel.

Where a recorded telephone line or another recorded voice messaging system is used for reporting information on breaches, verbal reports may be documented either by storing a recording of the conversation or by drafting a complete and accurate transcript of the conversation, which is to be shared with the Reporting Person to check, rectify and/or agree with.

Where an unrecorded telephone line or another unrecorded voice messaging system is used, verbal reports may be documented in the form of accurate minutes of the conversation, written by the staff members responsible for handling the report. The draft minutes are to be shared with the Reporting Person with a request to review and ultimately sign-off on.

Where a physical meeting is requested by the Reporting Person, such meetings may be documented by making a recording of the conversation or through accurate minutes prepared by staff members responsible for the handling of the report. The draft minutes are to be shared with the Reporting Person with a request to review and ultimately sign-off on.

***

[4] Recording keeping requirements in Germany are in general safeguarded by the Ombudsman (acting as the local Internal Alert System) and, where appropriate, by local branch functions.