



# Whistleblowing Policy



|   |   |
|---|---|
| I. Purpose and rationale of the Whistleblowing Policy.....  | 4 |
| II. Legal framework and aim of the Policy.....  | 4 |
| III. To whom and how should Potential Breaches be reported ?.....   | 5 |
| IV.Reporting breaches in Good faith.....  | 7 |
| V. Employees protection in case a (potential) breach is reported.....                                     | 7 |
| VI. What happens after the internal investigation ?.....  | 7 |
| VII. How will records related to Potential Breaches be stored and for which period of time ?.....         | 8 |
| VIII.External reporting channels: can employees also report Potential Breaches directly to the NBB ?..... | 8 |
| IX. Policy enforcement.....   | 9 |



## I. Purpose and rationale of the Whistleblowing Policy

UniCredit supports an ethical culture and behaviour at all levels of the internal organization that requires compliance with applicable legislation. It establishes references and guiding principles complementary to the legal obligations which must guide the expected behaviour in a coherent manner in relation to the mission of the company and its fundamental values.

A person applying for a job on the basis of an employment relationship or another legal relationship constituting the basis for the provision of work or services or performing a function or performing a service is provided by UniCredit with information on this internal reporting procedure at the start of the recruitment procedure or negotiations preceding the conclusion of a contract.

Each employee is expected to adhere to the principles of personal integrity and professional excellence. He/she is also responsible for complying with the bank's internal regulations, policies and procedures and its fundamental values with regard to the optimization of its services, ethical conduct, respect and teamwork.

In view of the above, each employee is authorized to report, via a specific procedure, possible violations of laws, regulations and procedures that could harm UniCredit, its customers, its employees or, more generally, the public at large.

On the proposal of the Executive Committee, the aforementioned Whistleblowing Policy is adopted by the Board of Directors.

## II. Legal framework and aim of the Policy

The Whistleblowing Policy is drawn up in accordance with:

1. The Banking Law: Article 21, § 1, 8° (internal reporting of breaches);

2. Other laws:

2.1. Organic Law of the NBB: Article 36/7/1 (external reporting of breaches)

2.2. Law of 28 November 2022 on the protection of persons who report breaches of Union law or national law observed within a legal entity in the private sector (transposing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, which regulates the establishment of internal and external reporting channels and the handling of breach reports)

2.3. Circular NBB\_2021\_28 of 16 November 2021 transposing Guidelines EBA/GL/2021/05 of 2 July 2021 on internal governance;

2.4. NBB circular 2024\_15 on the external channel for reporting of breaches of the legislation



supervised by the NBB;

2.5. Polish Act of 14 June 2024 on the protection of whistleblowers and Polish Banking Law;

### 3. International reference documents:

3.1. Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (the 'Whistleblower Protection Directive');

3.2. Guidelines EBA/GL/2021/05 of 2 July 2021 on internal governance => paragraphs 132 to 140.

The aim of this Policy is:

1. to encourage each member of staff to report any actual or potential misbehaviour, illegal activity or breach of internal policies or laws, regulations, self-regulatory codes and procedures;
2. to facilitate an internal investigation procedure in respect of misbehaviour;
3. to ensure the rapid establishment and adoption of remedial actions required in order to correct the malfunctions.

This objective will be reinforced by the adoption of appropriate measures to protect staff from negative consequences against them following reports of possible misbehaviour made in good faith that apply to the Bank ("**Potential Breaches**").

## III. To whom and how should Potential Breaches be reported ?

When submitting a report, the information should include:

- Reporting a problem or report involves highlighting all of the events that could be useful for the effective investigation of it.
- The circumstances include:
  - the day
  - time
  - place
  - nature of the facts
  - the identity of the persons concerned
  - any other details necessary to demonstrate the respective shortcomings and responsibilities.



All reports of breaches declarations must be made preferably by sending a written document to the Head of Compliance/Chairman of the Board of Directors. They can also be made anonymously through a written letter to the Head of Compliance/Chairman of the Board of Directors without mentioning your name or via a notification in an email sent via an anonymised email address (ex. whistleblower12345@gmail.com), which can be easily created through an email address provider.

Reporting breaches can be done by sending an e-mail to a dedicated email address: [declarationswhistleblowing@unicredit.be](mailto:declarationswhistleblowing@unicredit.be)

The Head of Compliance/Chairman of the Board of Directors is the only person having access to this mailbox. The Head of Compliance/Chairman of the Board of Directors ensures that this channel is secured and not accessible by other staff. All data related to the report will be handled in accordance with GDPR.

In the event of a report of Potential Breach concerning a member of the Compliance department, the email must be sent directly to the Chairman of the Board of Directors.

In case an employee does not want to report in writing, a report can also be made orally, by means of a physical meeting or a telephone call. In such a case, the Head of Compliance/Chairman of the Board of Directors will draw up minutes of that conversation, which will be secured and treated confidentially as reports made in writing. In the case of an oral report, after receiving a draft transcript of the report at the meeting, the whistleblower may check, correct and approve the minutes of the meeting by signing them.

The Head of Compliance/Chairman of the Board of Directors has the obligation to investigate all cases of reported violations.

Violations or suspected violations will be treated confidentially. The Bank will keep the identity of the persons who submitted the facts also confidential as far as possible and insofar as the facts, if they appear to be correct after internal investigation, unless disclosure is required under national law in the context of further investigations or subsequent judicial proceedings.

The Head of Compliance/Chairman of the Board of Directors has the obligation to carry out preliminary verifications, investigations and internal controls in order to rule on the merits and reliability of the reported facts. He must obtain objective elements and reconstruct the facts.

In order to allow the investigation, the statements must relate actual facts and useful information. The Head of Compliance/Chairman of the Board of Directors may request additional information or further details from the person who made the information. He can also at any time suspend or stop an investigation if he finds the baseless nature of a denouncement when verifying the elements in his possession. In this case, the declaration will be archived.

The Head of Compliance/Chairman of the Board of Directors will acknowledge receipt of the reporting of a breach. In case of absence of the Head of Compliance/Chairman of the Board of Directors the acknowledgement of receipt shall be sent by the Deputy Head of Compliance/Board member replacing the Chairman of the Board of Directors.

The confirmation of receipt of the whistleblowers report is to be sent to the whistleblower within 7 days,



unless the whistleblower did not provide a contact address to which the confirmation of receipt should be sent.

Feedback to the whistleblower on the internal report may not exceed 3 months from the date of confirmation of receipt of the internal report or – in the event of failure to provide the confirmation of receipt – 3 months from the expiry of 7 days from the date of making the internal report, unless the whistleblower did not provide a contact address to which the feedback should be sent.

All reported breaches will be promptly investigated and appropriate remediation actions will be submitted to the Executive Committee as far as the investigation justifies.

During the examination of the file and the evaluation of the declared facts, the Head of Compliance/Chairman of the Board of Directors may, if he deems it necessary, propose to the Executive Committee to call on external auditors, consultants or other experts to assist him in his investigation and analysis.

Except for prejudice to legal obligations, the identity of the person who has reported an offense may not be revealed to the person likely to have committed it.

## **IV. Reporting breaches in Good faith**

Anyone who reports a violation or suspected violation must act in good faith and be able to identify facts and situations related to negligent, illegal, atypical or incorrect circumstances and behaviour in relation to the activity carried out.

An employee who reports a fact is required to specify whether he/she has a personal interest in relation to the fact reported.

Any false or misleading information is prohibited.

Good faith does not mean that a report must absolutely prove to be correct. It is allowed to report activity that is suspicious without having established with certainty that it is also actually inappropriate behaviour. However, manifestly unjustified accusations which prove to be false can be considered as a disciplinary offense and may give rise to disciplinary sanctions in accordance with labor laws.

## **V. Employees protection in case a (potential) breach is reported**

This Policy prohibits retaliation against an employee who makes a report, provides information or takes part in an investigation.

Employees who, in good faith, report acts of violation must not be harassed or retaliated against and no negative consequence should affect their work. Examples of negative consequences include demotion,



suspension, termination, dismissal, threats or any other form of discrimination. This list is not exhaustive.

Any employee who takes reprisals against a person who has reported a fact in good faith could be subject to sanctions up to the termination of his or her contract, in accordance with labor law.

## **VI. What happens after the internal investigation ?**

The Head of Compliance/Chairman of the Board of Directors communicates each report of significant violation of laws or Internal Regulations to the Executive Committee and to the Chairman of the Board of Directors, to the extent appropriate. The Whistleblower identity is kept anonymous.

The Head of Compliance/Chairman of the Board of Directors also has the obligation to keep the Executive Committee periodically informed, at least every six months, of the state of the investigations.

In addition, an information note concerning the operation of the whistleblowing system, the reported breaches received and the remedial actions taken must be included in the annual report relating to the Internal Control system.

## **VII. How will records related to Potential Breaches be stored and for which period of time ?**

The Head of Compliance/Chairman of the Board of Directors will retain for a period of 3 years after the end of the calendar year in which the follow-up actions were completed or after the completion of the proceedings initiated by these actions all the documentation relating to each reported Potential Breach and to the investigations carried out. The Head of Compliance/Chairman of the Board of Directors will ensure that records related to reported Potential Breaches are stored in a register in a secure manner and that access to the register is restricted to the largest possible extent.

The register includes:

- 1) the report number;
- 2) the subject of the violation of law;
- 3) the personal data of the whistleblower and the person concerned by the report, necessary to identify these persons;
- 4) the contact address of the whistleblower;
- 5) the date of the report;



6) the information on the follow-up actions taken;

7) the date of completion of the case.

## **VIII.External reporting channels: can employees also report Potential Breaches directly to the NBB ?**

If employees are of the opinion that making a report internally is not possible, not appropriate or not timely, they can also make a report directly to the local authorities:Belgium

More information about making a report directly to the NBB can be found here:

<https://www.nbb.be/en/financial-oversight/general/contact/report-breach>

A breach form report is made available at the above mentioned NBB website:

<https://www.bkms-system.com/bkwebanon/report/clientInfo?cin=S48nXY&c=-1&language=eng>

### **Poland**

For employees of the Polish branch, a report can be made directly to the Commissioner for Human Rights or a public body. This can be done by following the instructions listed on the following website: <https://bip.brpo.gov.pl/en/content/how-refer-your-matter-commissioner-human-rights>

### **Germany**

Whistleblowers may contact:

- BaFin

([https://www.bafin.de/EN/DieBaFin/Hinweisgeberstelle/8\\_Zugang\\_zur\\_Hinweisgeberstelle/ZugangHinweisgeberstelle\\_node\\_en.html](https://www.bafin.de/EN/DieBaFin/Hinweisgeberstelle/8_Zugang_zur_Hinweisgeberstelle/ZugangHinweisgeberstelle_node_en.html)),

- Ministry of Justice

([https://www.bundesjustizamt.de/DE/MeldestelledesBundes/MeldestelledesBundes\\_node.html](https://www.bundesjustizamt.de/DE/MeldestelledesBundes/MeldestelledesBundes_node.html)

) - Federal Cartel Office

([https://www.bundeskartellamt.de/DE/Kartellverbot/Anonyme\\_Hinweise/anonymehinweise\\_node.html](https://www.bundeskartellamt.de/DE/Kartellverbot/Anonyme_Hinweise/anonymehinweise_node.html))

We nevertheless encourage employees to use the internal reporting procedures first to the largest possible extent.



## IX. Policy enforcement

Anyone who, in order to prevent another person from making a report, prevents them from doing so or significantly impedes it, may be subject to a fine, restriction of liberty or imprisonment for up to one year.

If the perpetrator uses violence, unlawful threat or deceit against another person shall be subject to the penalty of imprisonment for up to 3 years.

Anyone who takes retaliatory action against a whistleblower, a person assisting in making a report or a person associated with the whistleblower may be subject to a fine, restriction of liberty or imprisonment for up to 2 years.

Anyone who reveals the identity of a whistleblower, a person assisting in making a report or a person associated with the whistleblower may be subject to a fine, restriction of liberty or imprisonment for up to one year.

Anyone who makes a report or public disclosure knowing that no violation of the law has occurred may be subject to a fine, restriction of liberty or imprisonment for up to 2 years.

Aside from the above, same persons may be subject to disciplinary actions up to and including immediate dismissal and termination of the (employment) relationship