Whistleblower Policy
Banca Transilvania

Table of Contents

Introduction....2
Objective....3
Scope....3
Principles....4
Definitions....4
Reporting channels....6
Internal reporting channels....6
External reporting channels....6
Reporting Content....7
Reporting officer....7
Reporting Money Laundering/Terrorist Financing Violations....8
Protection of personal data....9

Introduction

The Whistleblower Policy (hereafter “WBR Policy”) supports the bank's commitment to an effective management, making it vital for managers and employees to adhere to the highest

ethical standards in fulfilling their professional responsibilities, while balancing the legitimate interests of the Group (hereafter “GFBT”) with the fundamental rights of employees.

The WBR Policy applies to the GFBT employees who report situations of breaches of internal regulations or legal provisions in force, including the legal provisions set out in *Annex No. 2 of Law 361/2022* or those of the specific AML legislation, *Law 129/2019 on the prevention and combating of money laundering*, and who have obtained the information on these violations in a professional context.

The principles and rules set out in the Policy are intended to encourage not only the employees but also any party with whom BT has a business relationship, such as contractors, subcontractors, and suppliers, to report in *good faith* based on information obtained during the recruitment process or pre-contractual negotiations.

Objective

In line with the Group’s values, we have created the necessary framework for the implementation of an internal *whistleblowing mechanism* for the reporting of *legitimate and substantive concerns* so they can be address without fear of any adverse consequences or retaliation.

We have always encouraged and provided the necessary information for reporting purposes if such *concerns* address situations of internal regulations or legal provisions violations, including the those set out in Annex 2 of Law 361/2022.

One major objective of the WBR policy is to protect the *whistleblowers* who report, ensuring the *confidentiality* of information and the security of persons making such reports to keep them safe against any direct or indirect reprisals.

Scope

This Policy applies to employees and any parties interacting in a business relationship with the bank. The whistleblowers will be advised to identify themselves, both to avoid abuse, and to allow for effective protection. This will also permit for better handling of the referrals should additional information be required. If an anonymous referral is still received, *anonymity is protected*, and the bank will proceed to deal with it in accordance with the provisions of the WBR Policy.

All employees must report any incident, any actual criminal, unethical conduct, or misconduct, including breaches of law. It should be noted that a person in managerial position may not use

their status to prevent another employee from exercising their rights or fulfilling their obligations under this Policy.

To ascertain that all complaints are legitimate and fall under the scope of this policy, the received referrals will be individually assessed. Should the complaints refer to any other type of matter (e.g., labor laws, IT matters,) they will be redirected to the appropriate channel.

Principles

The main principles falling under the scope of the WBR Policy:

- **1. The principle of legality,** according to which GFTB entities have an obligation to respect fundamental rights and freedoms by ensuring full respect for, inter alia, freedom of expression and information, the right to protection of personal data or the right of defense.
- **2. The principle of accountability**, according to which the person making the report has an obligation to provide data or information on the reported facts.
- **3. The principle of good faith,** according to which a person who had reasonable grounds to believe that the information concerning the reported violations was true at the time of reporting and that the information fell within the scope of Law 361/2022 is protected. A person who reports in bad faith and intentionally relies on false or misleading information is not protected under this Policy.
- **4. The principle of impartiality**, according to which the examination and resolution of reports is carried out without subjectivity, regardless of the beliefs and interests of the persons responsible for the resolution.
- **5. The principle of equality for all employees**, without discrimination based on sex, sexual orientation, genetic characteristics, age, nationality, race, color, ethnicity, religion, political choice, social origin, disability, family status or responsibility, membership or trade union activity.
- **6. The principle of confidentiality**, according to which reports are received, examined and dealt with confidentially.

Definitions

Stewardship framework is the essential component of corporate governance, which focuses on the internal structure and organization of the bank.

The Bank's organizational structure is set out in the BT Organizational Chart. The strategic management of the Bank is provided by the General Meeting of Shareholders, and the hierarchical management structure is provided by the Board of Directors and the senior

management bodies (the bank's Leaders' Committee/Managers), and that of the Group entities in their organizational charts.

Whistleblower/whistle-blower/whistle blower is a person, often an employee, who reveals information about activity within a private or public organization that is deemed illegal, immoral, illicit, unsafe, or fraudulent.

The Whistleblower Reporting Officer is an employee who has been appointed to manage whistleblower concerns confidentially. They will advise any employee who is the subject of a disclosure report about the disclosure if and when required to ensure procedural fairness and prior to any actions being taken or adverse findings being made.

Reporting is the communication of information obtained in a professional context, carried out for the purpose of preventing the materialization of potential events or the disclosure of events that have already materialized, which relate to the conduct of the Group's business of and/or the management of its entities or network and which constitute breaches of internal regulations and/or legal provisions, including the legal provisions set out in Annex 2 of Law 361/2022.

Anonymous reporting is the reporting that does not contain information allowing the identification of the whistleblower (name, position, e-mail address, etc.).

Reporting person is a member of the Group or, where applicable, another person, who makes a report under this Policy.

Retaliation is an action or omission, direct or indirect, occurring in a professional context, which is prompted by internal reporting, and which causes or is likely to cause harm to the reporting person.
Concerns include, without being limited to undesirable behavior money laundering and terrorist financing, violation of huma rights, theft, fraud, bribery, corruption.

My Alert is a special communication channels, available to GFBT employees or, where appropriate, to other persons who may report, signal, in confidence and without fear of retribution, legitimate and substantive concerns about issues relating potential fraud, possible breaches of the *BT Financial Group Code of Ethics and Conduct,* of the *Internal Rules of Procedure*, as well as violations of the law, including the legal provisions set out in Annex 2 of Law 361/2022.

Breaches of the law are considered acts consisting of an action or inaction that constitutes non-compliance with legal provisions, concerning the areas of financial services, products and markets, as well as the prevention of money laundering and terrorist financing, consumer protection or personal data protection.

Reporting channels

Internal reporting channels

To carry out internal reporting under conditions of confidentiality, the following internal channels are available to GFBT staff:

- **myalert@btrl.ro** - a dedicated email address that allows for confidential reporting of legitimate concerns by personnel or others who are entitled to make such reports. Each case received will be reviewed by members of the Alert Group (CEO, Deputy CEO, CRO, Senior Executive Director Corporate Governance and Litigation) and, if it qualifies under this policy, it will be assigned for investigation by inclusion into the specific application. Messages can be sent both from an internal e-mail address, as well as external. The sender receives a reply message with a unique reference code which he can use to track the status of his report.
- **My Alert internal application**. This method is based on a web application available on our *Intranet* page. The application allows for the confidential transmission of a report, each alert being assigned a unique reference code used to track the status of the report.
- **Face-to-face meeting** at the request of the whistleblower, using myalert@btrl.ro. Within a maximum of 7 days after the request, the proposed date and location will be sent to the reporting person. At the meeting, a designated person from the Corporate Governance and Litigation Department will record the report in an accessible form, subject to the consent of the person making the report.

External reporting channels

Banca Transilvania clients

Banca Transilvania has made available to its clients through its website an email address myalert@btrl.ro (link) through which any person who is not part of the GFBT group is able to communicate information obtained in a professional context to prevent the materialization of potential events or to disclose details of events that have already materialized, which relate to the conduct of GFBT's business and/or the management of BT's entities or the network and which constitute violations of internal regulations and/or legal provisions, including the legal provisions set out in Annex 2 of Law 361/2022;

All reports are handled in a confidential manner and in accordance with current regulations. Persons making a report are granted protection against the risk of reprisals, as provided for by the legislation in force. Any abuse of the whistleblowing system may expose the person reporting to disciplinary sanctions or criminal prosecution. However, using this system in good faith will not expose the whistleblower to any sanction, even if the facts are later found to be inaccurate or do not give rise to any prosecution.

Banca Transilvania staff

The GFBT staff will also be able to carry out external reporting as required by law. In this case, external reporting will be carried out using the channels made available to them by the authorities competent to receive such reports and carry out subsequent actions (e.g. National Bank of Romania, Financial Supervisory Authority).

Reporting Content

The report shall include the name and surname, contact details of the person making the report, the professional context in which the information was obtained, the concerned person, if known, a description of the fact likely to constitute a breach of internal regulations or the law within the GFBT, evidence in support of the report, if any, and the date and signature in the case of a face-to-face report.

As an exception to the above, reports that do not include the name, surname, contact details or signature of the person shall be examined and resolved to the extent that they contain substantiated indications of violations of internal regulations or the law.

In addition, the reported information must be of sufficient quality, in terms of volume and level of detail, to present a clear a picture of the raised issues. Also, it should comply with the principle of minimization of personal data provided for by the GDPR, as such only appropriate, relevant, and necessary personal data should be processed.

In view of specific legal regulations, reports received directly from employees of subsidiaries of BT Asset Management SAI and BT Capital Partners will be redirected to their own reporting channels, i.e. MyAlertBTAM@btam.ro and myalert@btcapitalpartners.ro, to be handled according to their own internal regulations.

Reporting officer

The Whistleblower Reporting Officer is responsible with:

- Receiving, examining, and forwarding the reports to the competent organizational structure for resolution.
- Liaising with the whistleblower, request additional information, and provide feedback within a reasonable period.
- Maintaining information and the identity of the person who filed the report confidential, as well as any other information that may lead directly or indirectly to their identification. Access to information processed in the framework of investigations must be granted strictly on a need-to-know basis.
- Disclosing information to other persons only if there is a legal basis under the applicable legislation.
- Making sure that the personal data and confidential information found during investigations is securely stored. Any personal/confidential information related to complaints kept for statistical purposes are anonymous.

Should an Executive Director/Senior Executive Director/BOD, Leader's Committee member be involved, prior to the initiation of the verification, the Chairman of the Board must be informed, and a person designated to carry out the verification and subsequent actions will be appointed.

The Corporate Governance and Litigation Department will draft a summary analysis of all warnings registered and incidents investigated at the level of the Group, as follows:

- annually to the Board, in the first quarter of the following year. The Board will endorse the annual report and adopt, if necessary, global measures required for the Group.
- quarterly to the Leaders' Committee.
- whenever appropriate to the Management Committee - if alerts are of high significance and incidents are reported which may seriously affect the reputation of the Group
- whenever necessary to the National Bank of Romania - Supervision Directorate, in case of legitimate and substantial concerns, likely to affect the safety, soundness and reputation of the bank.
- at the express request of the Chairperson of the Board of Directors, the Audit Committee, or other appropriate internal bodies.

The outcome of the verification shall be presented to the Alert Group members in the form of a report containing all information regarding the denial or confirmation of the reported incident and related problems, as well as the necessary recommendations to facilitate a favorable outcome.

Reporting Money Laundering/Terrorist Financing Violations

To adequately protect the personnel within the bank responsible for the fight against money laundering, we have implemented mechanisms so they can directly address to the supervisory

authority, to report violations of any kind of the *Law no. 129/2019 for the prevention and combating of money laundering and terrorist financing.* This mechanism will be used in all cases where the reports refer to one of the Alert Group members or to the Chairman of the Board.

To this end, in addition to the internal warning mechanisms mentioned in this Policy, the website of the National Bank of Romania provides, at the following link http://www.bnr.ro/Semnalarea-incalcarilor-Legii-nr.129-din-2019--23032.aspx, the necessary tools and information, respectively:

- a link to the online reporting form, and
- the possibility of connecting to the e-mail address dedicated to this issue *sesizari_AML@bnro.ro*

The National Bank has put in place mechanisms to protect whistleblowers through procedures for processing reports that guarantee confidentiality.

In addition, legitimate concerns about the Bank's actions in the area of money laundering can be reported to the National Office for the Prevention and Combating of Money Laundering, using the e-mail address: onpcsb@onpcsb.ro

Protection of personal data

All investigations and reports are carried out in a strictly confidential manner, in compliance with the legislation in force as well as with the internal regulations of GFBT, including the identity of the data subject during the checks.

Personal data collected because of reporting under this Policy, or the law may be disclosed, as appropriate to bank who have the right and need to know access and to the authorities, where such disclosure is necessary for the conduct of any subsequent criminal or judicial proceedings.