Whistleblowing Policy

Optima bank S.A.

13.01.2023

Optima bank S.A. Regulated by the Bank of Greece License No: 52/2/17.12.99
Registration Number of Hellenic Business Registry: 003664201000 • LEI Code: 2138008NSD1X1XFUK750
Tax Registration No: 099369013, Tax Procedures and Service Provision Center of Attica
32 Aigialeias Str & Paradissou, 151 25 Maroussi • Tel. +30 210 81.73.000 • Fax. +30 210 81.73.101
optimabank.gr

CONTENTS

1. Introduction

Whistleblowing is an intentional disclosure recorded in the files Bank and its subsidiaries (Hereinafter called "the Group") and conducted by a person who is aware of, either significant misconducts and omissions or other offensive acts, actual, potential or imminent within the Group.

The Bank of Greece Governor's Act 2577/9.3.2006 sets out the obligation to establish a framework for anonymous reporting and for the protection of employees who, through such reports, inform the Board of Directors or the Audit Committee or the Internal Audit Directorate of serious misconducts, omissions or offensive acts that have come to their attention.

The European Parliament and the Council have issued Directive (EU) 2019/1937 "on the protection of persons who report breaches of Union law". The purpose of the Directive is to strengthen the enforcement of Union law and policies in specific areas by establishing common minimum standards to ensure a high level of protection for persons reporting breaches of Union law. The Directive was transposed into national legislation by the Law 4990/2022 (Government Gazette Issue I, No 210/11.11.2022) therefore references to articles of the Directive in this Policy correspond to respective articles of the above national Law.

This Policy is established, approved and supervised by the Executive Committee of the Bank as the parent company of the Group, and at the same time ensures the protection of persons making disclosures and reports. This Policy is applicable and binding for all Group companies.

2. Purpose

The purpose of the Policy is to:

- ✓ Establish rules that will facilitate and encourage any Group stakeholder (as defined below) and any third party to submit named or anonymous reports about serious misconduct, omissions or offensive acts brought to their attention in order to protect the reputation and integrity of the Group and its employees.
- ✓ Preserve the confidentiality of the identity of persons making such reports, and their protection.
- ✓ Provide the stakeholder with guidance on how to raise their concerns within the Group.
- ✓ Reassure the stakeholder that they can raise genuine concerns without fear of retaliation, even if those concerns turn out to be wrong.
- ✓ Contribute to the enhancement of integrity, transparency, accountability and the identification and adoption of appropriate corrective and/or repressive measures, as well as the protection of both the employees and the Group.
- ✓ Define the principles and framework of managing and investigating of whistleblowing reports within the Group.

3. Key Concepts – Definitions

- ✓ "Stakeholder": (often referred to as Participant, Social Stakeholder, Social Partner, Involved Party, or Stakeholder Groups) refers to all those affected by the Group's activities. The most known stakeholder groups are: employees, shareholders, Group executives, customers, suppliers, consultants, subcontractors, contractors and all kinds of partners, etc.

- ✓ "Types of misconducts": acts or omissions that are illegal and related to the Group's activities or contradict to the purpose or scope of the rules and policies established by the Group. Indicative cases are described in Section 5.
- ✓ "Report" or "to report" means, the oral or written communication of information on breaches.
- ✓ "Reporting person" means a natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities or relationship with the Group.
- ✓ "Person concerned" means a natural or legal person who is referred to in the report as a person to whom the breach is attributed or with whom that person is associated.
- ✓ "Retaliation" means any direct or indirect act or omission which occurs in a work-related, business or customer context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person.
- ✓ "Malicious report": A report made with the knowledge of the reporting person that it is not true.
- ✓ "Good faith / bona fide": Reasonable belief by the reporting person, based on the circumstances and the information available to them that the information provided are true.
- ✓ "Sensitive personal data": This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed solely for the purpose of identifying an individual, data concerning health, data concerning the sexual life or sexual orientation of an individual.
- ✓ " Whistleblowing Management Committee" (hereinafter referred to as the "WMC"): The Committee which is responsible for the management and investigation of the Whistleblowing reports and which consists of **regular** and substitute members and reports to the Audit Committee of the Board of Directors of the Bank. The **regular** members of the WMC are the following Heads of the Bank's Divisions:
  - Internal Audit (hereinafter referred to as the IAD)
  - Compliance
  - Risk Management
  - Legal
  - Human Resources

  The Head of Internal Audit presides over the WMC.
- ✓ Reporting channels: The internal communication channels through which reports are submitted

4. Types of offensive acts

Reports of misconduct, omissions or offensive acts include, but are not limited to, the following cases:

- theft/embezzlement
- fraud
- corruption/bribery

- Asset misappropriation
- breach of banking secrecy
- misleading presentation of data
- abuse of power
- violation of the Group's policies
- violation or behaviours that harms the reputation or scope of the Bank and the Group companies
- violation of the legal and regulatory framework
- human rights violations and discrimination
- other unethical behaviour
- deliberate concealing of information about any of the above

The Policy does not cover:

- customer complaints regarding the quality of the services provided by the Group
- disagreements on matters concerning policies and decisions of the Group companies

Management

- personal issues and disagreements between colleagues or supervisors
- rumours

5. Key Principles

The key principles underlying this policy are the following:

- ✓ The Group encourages the submission of named or anonymous reports regarding serious misconduct, omissions or offensive acts brought to the attention of any employee, regardless of hierarchical level, and any third party, using any communication channel he/she deems appropriate.
- ✓ However, anonymous reports can make it difficult or even impossible to investigate and assess the credibility of the report. People who have reported or disclosed information on breaches anonymously but who are subsequently identified and suffer retaliation are entitled to the protection provided for in Directive 2019/1937 (EU) if the conditions are met, pursuant to Article 6 par. 3 (Article 7 par. 3 of Law 4990/2022).
- ✓ The Group is committed to maintain the anonymity of the reporting person and other parties involved, and to refrain from actions that may result in the disclosure of their identity.
- ✓ However, it should be noted that disclosure of the identity of the reporting person may be required by judicial or legal proceedings as part of the investigation of the case.
- ✓ Reports will be examined with due diligence, impartial judgment and objectivity and if the allegations are confirmed, the Group is obliged to take all appropriate corrective measures. Anonymous reports are investigated according to the quality of their documentation and the ability of identifying the misconduct reported.

- ✓ Reporting person who have made a report in good faith shall be protected from any acts of retaliation, discrimination or other forms of unfair treatment, regardless of the outcome of the investigation of the report.
- ✓ The reports are made without the promise of payment or the existence of any consideration. If the reporting person was involved in the event, will not be absolved of responsibility but his /her contribution to the detection and investigation of misconduct, omissions or offensive act will be taken into account.
- ✓ The Group respects the fundamental rights of the persons involved in a report and ensures that the actions and procedures provided for are in accordance with the applicable legislation.
- ✓ The rights and remedies laid down in Directive 2019/1937 (EU) are not waived or limited by any individual agreement, policy, form or term of employment.

6. Reporting illegal activities and policy breaches

It is recommended that the following guidelines and instructions be followed when reviewing and investigating a report:

- ✓ The reporting of the misconduct should be done in good faith and without delay, as soon as it becomes known to the interested party.
- ✓ The report should be clear, specific and contain as much information and detail as possible to facilitate its investigation.
- ✓ The report should include at least the name of the person(s) who may have committed a misconduct, the date/time period and place where the incident took place, the Group company to which the incident pertains, the type of misconduct and the most detailed description possible.
- ✓ Personal data, including sensitive data, and more generally information that are not related to the incident should not be included in the report. If they are included, they shall be deleted.
- ✓ The reporting person does not need to be absolutely certain of the validity of their report. As long as they have reasonable concerns or suspicions. They should not engage in illegal actions that may place them, the company/Group or a third party, at risk in order to seek and collect more information to support their report.
- ✓ The submission of named confidential reports is encouraged so that communication is possible and more information is provided if requested and necessary. However, it is made clear that anonymous reports are treated with exactly the same attention and weight as named reports.
- ✓ Members of the Group's staff have a duty to report any action or breach that comes to their attention. Failure by a staff member to report illegal activity, breach of regulations or even suspected breach of the above, is an offensive act and will be treated as such.
- ✓ In case a Group employee or a third party has doubts about the need to report misconduct, omission or offensive act or suspicion thereof, or wishes clarification regarding their protection or other matters, and their questions are not covered herein, they can address to the Head of Internal Audit Division for guidance.

- ✓ The Group has designated the following dedicated reporting communication channels which are available all days and hours of the week and **can be used to submit** both named and anonymous reports.
  - **By mailing a letter, named or anonymous to P.O. Box No. 61371 that the Group maintains at Hellenic Post (ELTA) of MAROUSSI,**
  - **By e-mail to the dedicated e-mail address of the Bank (whistleblowing@optimabank.gr)**
- ✓ The above communication channels are available all days and hours of the week, are routed to the Bank's Head of Internal Audit (IAD) and then submitted to the WMC.

7. Protection against possible acts of retaliation

The Group prohibits retaliation of any kind against a reporting person who has made a report in good faith.

In accordance with Article 19 of Directive 2019/1937 (Article 17 of Law 4990/2022) as retaliation are indicatively:

- suspension, dismissal or equivalent measures,
- demotion or withholding of promotion,
- transfer of duties, change of location of place of work, reduction in wages, change of working hours,
- withholding of training,
- a negative performance assessment or employee reference,
- imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty,
- coercion, intimidation, harassment or ostracism,
- discrimination, disadvantageous or unfair treatment,
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment,
- failure to renew, or early termination of, a temporary employment contract,
- harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income,
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry,
- early termination or cancellation of a contract for goods or services.

The Group protects all those who report in good faith **unlawful behaviour**s. In this context, any kind of negative **treatment**r against anyone who has made a report is prohibited, even if the report is subsequently proven to be incorrect.

The same level of protection applies to third parties connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons.

If the reporting person is an external partner, early termination or cancellation of a contract for goods or services as a result of the report is prohibited.

8. Complaints management procedure

The Group maintains a registry of the submitted reports and a record of the related documents. The register and the relevant records are kept for 5 years unless other legal reasons require their retention and in accordance with the Group's policies. In any case, reports are stored for a reasonable and necessary period of time in order to be retrievable and to comply with the requirements of the law and in any case until the completion of any investigation or judicial proceedings initiated as a consequence of the report against the person concerned, the reporting person or third parties (Article16 par. 1 of Law 4990/2022).

Responsible for receiving, investigating, registering and keeping records of the reports, at all levels and for all Group companies, is the Bank's Head of Internal Audit (IAD).

In case of a named report:

- Is ensured that the confidentiality of the identity of the reporting person and any third party named in the report is protected and that unauthorised staff members are prevented from accessing it (need to know principle),
- The IAD shall inform the reporting person by fixed means of the receipt of the report within seven working days of the receipt of the report by the Group.

The reporting person will receive an update on the progress of their report within a reasonable period from the receipt of the report, which shall not exceed three months from the acknowledgement of receipt, from the IAD. If no acknowledgement of receipt has been sent in accordance with the previous paragraph, the period shall be three months from the end of the seven-day period following the submission of the report.

9. Personal Data

Any processing of personal data under this policy, including the exchange or transmission by the competent authorities, shall be carried out in accordance with national and European data protection law, including any specific legislative provisions and the harmonised data protection policy of the Group, which shall take all necessary technical and organisational measures to protect personal data.

The personal data of all parties involved are protected and processed solely in relation to the report and for the sole purpose of verifying the validity or otherwise of the report and investigating the specific incident. Personal data that are not directly related to the report or are excessive are not collected or, if collected accidentally, are deleted without undue delay.

Only those involved in the management and investigation of the incident can have access to the data contained in the reports.

The Bank, as the Controller, by derogation from case (a) of par. 1 of Article 5, Articles 12 and 13, par. 1 to 4 of Article 14 and Article 34 of the General Data Protection Regulation does not provide relevant information on the processing of personal data to the reporting person and any third party in their capacity as data subject, named in the report or the personal data resulting from monitoring measures and in particular on the source of origin in accordance with case (f) of par. 2 of Article 14, pursuant to par. 5 of the same Article in conjunction

with Article 23 of the General Data Protection Regulation for as long as necessary and if deemed necessary for the purpose of preventing and countering attempts to obstruct reporting, obstruct, cancellation or delay in monitoring measures, in particular with regard to investigations or attempts to identify the reporting persons, as well as to protect them against retaliation.