Whistleblowing Policy

1. Introduction

The OPAP Group of Companies (collectively "the Group") is committed to ensure the highest level of ethical and professional conduct and zero tolerance to illegal or irregular actions, which affect the Group's reputation and compliance with its legal and regulatory obligations.

For the purposes of this Policy, the OPAP Group of Companies includes subsidiaries established in Greece (namely, Hellenic Lotteries S.A., Horse Races S.A., Neurosoft S.A, TORA Wallet S.A., TORA Direct S.A.), and in the Republic of Cyprus (OPAP Cyprus Limited and OPAP Sports Limited) (hereinafter each of them referred to as the "Group Company" and together the "Group Companies").

The Group encourages its employees and associates to promptly report any violations of the law and incidents of misconduct. This is the only way in which the principles and values of the Group and the rules of lawful, ethical and professional conduct can be safeguarded and will continue to be applied, while ensuring that the Group will be able to take any corrective action(s) required.

2. Purpose

The purpose of the Whistleblowing Policy (**Policy**) is two-fold: **(i)** to allow the Group to comply with Greek Law 4990/2022 **(the "Whistleblowing Law" or "WB Law")** and the Cypriot Whistleblowing Law **(the "Cypriot WB Law")**, both transposing Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law (the **"Whistleblowing Directive" or "WB Directive"**) into Greek and Cypriot legislation respectively, and **(ii)** to provide a framework for the timely detection of misconduct within the operations of the Group and each Group Company.

This Policy also sets out the principles, protection measures and general operational framework under which the Group Companies receive, manage, and investigate reports of illegal acts or misconduct, which relate to them and have come to the attention of their employees or third parties.

In principle, this Policy aims to:

I. Encourage people to report suspected misconduct as soon as possible, in the knowledge that their reports will be taken seriously and investigated as appropriate, with confidentiality as a principal focus.

II. Provide people with guidance as to how to submit those reports.

III. Reassure people that they should be able to raise genuine concerns in good faith, without fear of retaliation.

[Business/Internal Use]

3. Definitions & Abbreviations

Report	Report submitted by a person via the designated Reporting Channels regarding a breach of law or misconduct falling within the scope of this Policy
Reporting Channel(s)	The hereby designated channels for submitting a Report
Reporting Person	Person who files a Report via the available Reporting Channels
Reported Party	A natural or legal person who is referred to in a Report as the person to whom the breach is attributed or with whom that person is associated
RAMR	Responsible person for the acceptance and monitoring of Reports
Deputy RAMR	Responsible person for the acceptance and monitoring of Reports, in case the RAMR is unable to handle the case (due to conflict of interests etc.)
NTA	National Transparency Authority
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)
The Cypriot Whistleblowing Law	Law 6(I)/2022 of the Republic of Cyprus on the protection of whistleblowers of National and Union Law

4. Personal Scope

This Policy applies to:

1. Persons who acquired information on a breach of law or misconduct in a work-related context, including at least the following:

   a) members of the Board of Directors (and of the respective Board Committees), as well as any shareholders of any Group Company,

   b) all employees of the Group Companies of all levels, irrespective of the type of their employment contract,

   c) self-employed persons, advisers or persons working from home,

   d) volunteers and paid or unpaid trainees of any Group Company,

   e) suppliers, contractors and sub-contractors of any Group Company, as well as persons employed by or working under the directions of the foregoing,

2. Persons (of any of the capacities referred to above under 1), who acquired information on a breach of law in a work-based relationship which has since ended.

3. Persons (of any of the capacities referred to above under 1), whose work-based relationship is yet to begin, where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

4. Intermediaries or third parties (natural or legal persons) that are linked to the Reporting Persons or their Report (*e.g.*, co-workers or relatives of the Reporting Person, legal entities that the Reporting Person owns or works for).

5. Material Scope

5.1 Violations covered by this Policy

The prompt submission of Reports via the designated Reporting Channels is encouraged, if a person thinks s/he has any information relating to incidents concerning the Group Companies' activities in one (or more) of the areas that follow.

It is noted that Group A Violations are those provided for in the WB Directive and the national WB Laws (in Greece and Cyprus), whereas Group B Violations are cases of misconduct which, though not covered by the WB Directive and the national WB Laws, constitute cases of serious misconduct, the reporting of which the Group also wishes to encourage. However, it is underlined that the specific protection measures for Reporting Persons stipulated in the WB Directive and the national WB Laws shall apply solely in cases of Reports of incidents of Group A Violations. In particular:

Group A (the "Group A Violations")

1. Violations falling within the scope of European Union (EU) acts set out in Part I of the Annex of the WB Directive and Part I of the Annex of the Greek WB Law, which specifically relate to the objectives and operations of the Group Companies in any of the following areas:
   - Public procurement,
   - Financial services, products and markets,
   - Prevention of money laundering and terrorist financing,
   - Product safety and compliance,
   - Protection of the environment,
   - Food and feed safety,
   - Public health,
   - Consumer protection,
   - Protection of privacy and personal data, and
   - Security of network and information systems.
2. Fraud and any other illegal activity affecting the financial interests of the EU, as referred to in Article 325 TFEU.
3. Violations relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of EU competition and state aid rules, as well as corporate tax law breaches.
4. Violations falling within the scope of the EU acts set out in Part II of the Annex of the WB Directive and Part II of the Annex of the WB Law, to the extent that no specific whistleblowing provisions

apply, as long as such acts are applicable to the operations of the Group Companies, especially in the following areas:

- Statutory audits of the annual financial statements (stand alone and consolidated),
- Market Abuse Framework, including any incomplete or inaccurate public disclosures made by the Group,
- Prospectus Regulation (Reg. EU 2017/1129) on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market),
- Legal framework applicable to Group Companies offering financial services and products and framework related with prevention of money laundering and terrorist financing.

5. Only with respect to the Group Companies *established in the Republic of Cyprus,* breaches of the applicable Cypriot legislation which may concern:
   - Committing a criminal offence,
   - Violations of legal obligations imposed by the laws and/or regulations of the Republic of Cyprus,
   - Violations that endanger or are likely to endanger the safety or health of any person,
   - Violations that cause or are likely to cause damage to the environment.

Group B (the "Group B Violations")

1. Violations of any other law, rule or regulation applicable to any Group Company, including the following:
   - Questionable accounting practices, violations of internal accounting controls, financial reporting irregularities or any other financial matters, such as fraud or deliberate error in the preparation, evaluation, review of any financial statement or in the recording and maintaining of financial records of the Group Companies.
   - Any behavior which may be defined as financial criminal offence or attempt thereof, such as fraud, embezzlement, bribery, corruption, forgery or alteration of documents.
2. Any misconduct, such as:
   - Abuse of power,
   - Misappropriation or misuse of Group Companies' resources,
   - Unauthorized disclosure of confidential information,
   - Conflict of Interests,
   - Infringement of Group Companies' IP rights,
   - Deliberate concealment of any of the above matters.

5.2 Other violations covered by other OPAP Policies

Reports related to human resources policies and processes are not covered by this Policy and should be submitted to the respective line manager and/or the Chief People Officer. Personal grievances, bullying, harassment or discrimination complaints should be submitted through other available internal channels, as per the ***Policy on Workplace anti-violence and anti-harassment P-185*** and ***Internal Complaints Management Procedure regarding violence and harassment incidents P-186***.

6. Internal Reporting Channels & RAMR

6.1 Internal Reporting Channels

OPAP S.A. has established the following internal Reporting Channels that shall also be used by the Group Companies, to the extent permitted by law. Reports may be submitted:

a. via the reporting platform, which can be accessed via the Company's intranet and website (e-platform),

b. by e-mail to whistleblowing@opap.gr,

c. by post to the OPAP S.A. or the relevant Group Company's address, marked as "Confidential" and only to the attention of the RAMR, or

d. directly to the RAMR, orally or in written form.

Each Report should include: the main cause of the Report (acts or omissions that may potentially cause or have caused a reportable incident), with specific information (e.g., names, dates, location) and substantiation through relevant documents or other records. It is not necessary to include evidence inside the Report submission, but any relevant information that will facilitate the assessment of the Report will be considered.

6.2 RAMR Designation & scope of activity

A. OPAP S.A.

The RAMR is central in the proper implementation of this Policy, as s/he is responsible for receiving and following up on Reports submitted via the designated Reporting Channels. The role of RAMR is entrusted with the **Corporate & Network Compliance Director** of OPAP S.A.

In case a conflict of interests arises in the handling of a specific Report, the RAMR shall be substituted by the Deputy RAMR. The role of Deputy RAMR is entrusted with the **RG & Corporate Compliance Manager** of OPAP S.A.

In cases where the Report reveals a structural (Group) problem or a problem that affects two or more Group Companies, the Report shall be handled by the OPAP S.A. RAMR.

B. Group Companies

The Group Companies may also appoint the aforementioned (under A) persons as their RAMR/Deputy RAMR, to the extent allowed by the applicable legal framework.

In both cases (under A or B), the RAMR/Deputy RAMR shall be supported in their duties by a dedicated team (as deemed necessary, depending on the size of the Group Company and the number of its employees) and shall report directly to each Group Company's Board of Directors.

C. Duties & Responsibilities

The RAMR (and, in case of substitution, the Deputy RAMR) shall have the duty to:

(a) provide appropriate information on the possibility of filing a Report and communicate the information in a prominent place within the Company's webpage,

(b) receive Reports falling within the scope of this Policy,

(c) make an initial assessment of the Report and lay the groundworks for the competent employees and executives to deal with the Report or terminate the procedure by archiving the Report if it is: i) incomprehensible, or ii) not sufficiently justified, or iii) clearly unfounded due to unreliable information, or iv) submitted in an abusive manner,

(d) engage any employee/corporate body of any Group Company, as deemed appropriate for the handling of the Report,

(e) ensure the protection of the confidentiality of the identity of the Reporting Person and any person(s) named in the Report in accordance with applicable legislation,

(f) monitor the process of the Report and maintain contact with the Reporting Person and, if necessary, request further information from the latter,

(g) inform the Reporting Person regarding the outcome of the investigation and the actions that have been taken, in accordance with applicable legislation,

(h) design and coordinate training activities on ethics and integrity, participate in the development of internal policies to enhance integrity and transparency within the Company.

7. RAMR & Reporting handling process for Group A Violation as per WB Law

In case of a Group A Violation, the Reporting Person may either file an Internal (under Section 7.1. below) or External Report (under Section 7.2. below). Public disclosure is afforded with the special protections of the WB Directive and the national WB Laws (in Greece and Cyprus), only under the conditions set out in Section 7.3 below.

7.1 Internal Reports

A Report for a Group A Violation may be filed through the internal Reporting Channels set out in Section 6.1. above. To the extent required by law, Group Companies shall establish in parallel additional dedicated reporting channels at a Group Company level.

It is noted that Reports filed via the e-platform will be received and handled by OPAP S.A. RAMR. The Reporting Person maintains the right to request that his/her Report is dealt with at the involved Group Company's level only, by explicitly stating so in the Report and by making use of the remaining internal Reporting Channels (under letters b-d of *Section 6.1*.).

7.2 External Report (applicable solely to Group A Violations)

Reporting Persons are encouraged to report any Group A Violations using the aforementioned Reporting Channels (internal reporting) rather than approaching competent authorities (external reporting), without prejudice to the right of every Reporting Person to file a Report directly with a regulatory authority or any other relevant state body deemed appropriate. In any case, the RAMR shall provide, upon request and according to the applicable legislation, assistance and access to any competent public, administrative or judicial authority during the investigation of such incident or conduct.

The external Report shall be submitted to the competent authorities, as prescribed by WB Law, and in particular:

(a) The NTA, which is the competent authority under the Greek WB Law, in case the Reporting Person has/had a working relationship with the Group Companies established in Greece; Reports to the NTA must be submitted via the means determined by such authority.

(b) Other independent supervisory authorities or public bodies competent to handle such Reports, such as the Hellenic Competition Commission for competition law violations (Articles 101 and 102 TFEU), the Hellenic Capital Market Commission for violations relating to Market Abuse Framework, the Bank of Greece for violations in the payments sector.

7.3 Public Disclosure (applicable solely to Group A Violations)

A person who makes a public disclosure concerning Group A violations shall not be entitled to protection in accordance with Section 8.2 below, unless one of the following conditions are met:

(a) the person first filed a Report internally and externally to the NTA, or directly only to the NTA, but no appropriate action was taken in response to the Report within three (3) months from its submission, or

(b) the person has reasonable grounds to believe that the breach in question may constitute a risk to the public interest, or where there is an emergency situation or a risk of irreversible damage, or, in case of a Report to the NTA, there is risk of retaliation, or there is little prospect of the infringement being effectively addressed, because of the particular circumstances of the case, such as where evidence may be concealed or destroyed or where any authority or body may be in collusion with the perpetrator of the infringement or involved in the infringement.

7.4 Handling of a Group A Violation Report – Additional Duties of the RAMR

In case of a Report concerning a Group A Violation, the RAMR, apart from the duties set out under Section 6.2. above, shall have the *additional* duties to:

(a) acknowledge receipt of the Report to the Reporting Person within seven (7) working days,

(b) inform the Reporting Person about the initial assessment of his/her Report by notifying the Person of any relevant decision,

(c) inform the Reporting Person on the actions that have been taken within a reasonable time period, which shall not exceed three (3) months from the acknowledgement of receipt or, if no acknowledgement has been sent to the Reporting Party, within three (3) months from the expiry of seven (7) working days from the submission of the Report, and

[Business/Internal Use]

(d) provide clear and easily accessible information on the procedures under which Reports may be submitted to the NTA and, where applicable, to public bodies or institutions or other bodies/agencies of the European Union.

8. Protection Measures for Reporting Persons

8.1 General Protection

The Group will take into consideration and will promptly and thoroughly investigate all Reports of potential misconduct (Group A and Group B Violations).

For persons reporting Group A Violations the special protections of the Greek WB Law, the Cypriot WB Law and the WB Directive will be afforded, as set out in detail in Section 8.2. below.

For Persons reporting Group B violations, protection will be afforded according to applicable legislation, depending on the nature of the reported violation.

In any case (Group A and Group B Violations):

(a) All Reports will be treated with confidentiality, unless disclosure is necessary under applicable legislation,

(b) All personal data will be processed in accordance with the GDPR and other applicable legislation regarding data processing,

(c) The Group will not tolerate retaliation against Reporting Persons who submit a Report in good faith,

(d) The Group shall keep the Reporting Person informed about the progress and outcome of the investigation, to the extent possible so that the conducted investigation is not jeopardized,

(e) Remedial actions will be taken depending on the nature and gravity of the misconduct or circumstances reported and the results of the investigation, in accordance with applicable legislation and the Company's policies and procedures.

8.2 Special Protection Measures for Group A Violations under WB Law only

Any Report of Group A Violations shall be treated in accordance with the provisions of Sections 8.2.1 to 8.2.3 below. It is noted that under the Cypriot WB Law, the special protections are afforded to a Reporting Person, provided s/he has filed their Report eponymously.

8.2.1 Confidentiality

A basic and inviolable principle of the Policy is to protect the identity and confidentiality of the Reporting Person and, if they are employees of the Group, to ensure their position and/or their professional development is not compromised. Therefore, the Group shall guarantee the confidentiality of the identity of the Reporting Person. However, the Reporting Person's identity will only be disclosed in the context of a legal obligation, as stated below.

All information relating to a Report will be treated confidentially and special technical and organizational measures (*i.e.,* pseudonymization) will be implemented. Such information and/or the

Reporting Person's identity (directly or indirectly) will not be disclosed to any unauthorized person/entity, except for when the Reporting Person provides his/her explicit consent for disclosure.

The obligation of confidentiality is also vested upon the Reported Parties, as well as any other person being named in the Report.

By way of derogation, any information relating to a Report, including the Reporting Person's identity, may be exceptionally disclosed without his/her consent and upon his/her proper, written notification in the following cases:

a. when it is required under national and/or European legislation,

b. in the context of an investigation by the authorities, or

c. in the context of judicial proceedings,

and only if this is necessary for handling the Report or to secure the defending rights of the Reported Party, as per applicable legal provisions.

The identity of the Reported Person is respectively protected during the follow-up on the Report.

The Group allows the submission of a Report through the established Reporting Channels of communication either eponymously or anonymously, as per applicable provisions. However, the Group encourages Reporting Persons to submit their Report by name, as it creates a better communication channel for both the provision of further clarifications and the follow-up on the Report.

As above mentioned especially with regard to Group Companies with corporate seat in the Republic of Cyprus, the applicable Whistleblowing Law in Cyprus requires the Reporting Person(s) to submit their Report eponymously, in order to receive the protection offered by the aforementioned Law.

8.2.2 No retaliation

The Group is committed to the protection of the Reporting Person, if s/he has submitted the Report in good faith and they have reasonable ground(s) to believe that their Report is true and falls into the subject-matter scope of the Policy. The same protection shall also be afforded to any intermediaries or third parties (natural or legal persons) that are linked to the Reporting Persons or their Report.

The Group will not tolerate any form of retaliation, nor threats or attempts thereof, in view of the Report, including:

(a) suspension, lay-off, dismissal or equivalent measures;

(b) demotion or withholding of promotion;

(c) transfer of duties, change of location of place of work, reduction in wages, change in working hours;

(d) withholding of training;

(e) a negative performance assessment or employment reference;

(f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;

(g) coercion, intimidation, harassment or ostracism;

(h) discrimination, disadvantageous or unfair treatment;

(i) failure to convert a temporary employment contract into a permanent one;

(j) failure to renew, or early termination of, a temporary employment contract;

(k) intentional harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;

(l) 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;

(m) early termination or cancellation of a contract for goods or services;

(n) cancellation of a license of permit;

(o) psychiatric or medical referrals; and

(p) refusal to or deprivation of reasonable adjustments to disabled persons.

Any such form of retaliation is considered a serious breach of the applicable laws and the present Policy and must be immediately reported to the RAMR through any of the available Reporting Channels.

The Group acknowledges that the Reporting Person has access to appropriate remedial measures and specifically:

(a) the right of full compensation for any form of retaliation;

(b) the right to request restoration to the previous situation before the prohibited retaliation actions; and

(c) the right to be protected from any form of retaliation, such as the termination of the employment contract, which in any case shall be deemed void.

8.2.3 Personal Data

The processing of personal data included in the Reports and respective follow-up/investigation proceedings, is carried out in accordance with national and European legislation regarding personal data protection and the relevant policies and privacy notices of the Group.

In particular:

The personal data of all parties involved in the Report are protected and processed solely in the context of prevention, detection or investigation of irregular, unethical, illegal or criminal behavior.

Only the RAMR and those involved in the investigation of a given Report can access the data contained in said Report. In particular, the recipients of personal data included in the Report may be the Group's competent persons (employees, executives or Units), *e.g.,* the Data Protection Officer, the Audit Committee, the Board of Directors, external consultants bound by confidentiality clauses, lawyers, the provider of the e-platform, as well as judicial and/or administrative authorities.

The Group will retain personal data for a certain time period following the completion of the investigation, which might vary depending on the outcome of the investigation. For instance:

- If the Report is deemed unfounded, the personal data shall be deleted within three (3) months from the date of its filing.
- If the reported situation follows judicial recourse, the personal data shall be erased upon issuance of the respective final court decision.
- If the Report results in substantiated findings against an employee, officer or executive of the Group, the personal data shall be retained for the duration of his/her employment/relationship with the Group and shall be deleted twenty (20) years after the termination of the cooperation.
- If the Report results in substantiated findings against an external partner, vendor, contractor or supplier of the Group, the personal data shall be retained for the entire duration of his/her cooperation and shall be deleted five (5) years after the termination of such cooperation.

In any case, the responsibility of retaining/deleting any personal data contained in a Report and/or gathered in the investigation process that shall follow, lies with the RAMR, who shall act in consultation and cooperation with the Data Protection Officer.

The Group implements the necessary technical and organizational measures to ensure a high-level data security (such as access to information “on a need-to-know basis”, imposing confidentiality obligations to the personnel who has access, monitoring accesses and access rights, use of encryption, keeping passwords confidential, etc.).

The Reported Parties and any other persons named in the Report, shall not be informed about the processing of their personal data as normally required under applicable data protection legislation, for as long as necessary, in order to prevent any attempts to obstruct the handling of the Report or retaliation measures. Accordingly, any data subject requests exercised by any Reported Parties or relevant named persons, may not be satisfied. In case of doubt, the Data Protection Officer, who receives the data subject request, decides on an ad hoc basis.

9. Sanctions under the WB Law (applicable only in relation to Group A Violations)

A person may be subject to imprisonment and/or financial penalty if s/he:

(a) obstructs or attempts to obstruct the reporting of violations falling within the scope of this Policy,

(b) retaliates or instigates malicious proceedings against the persons referred to in Section 4 of the Policy, or

(c) violates the obligation to maintain the confidentiality of the identity of the Reporting Person(s).

In calculating the penalty, account shall be taken of the intensity of the retaliation and the gravity of the infringement.

If any of the above violations has been committed, for the benefit or on behalf of a legal entity, an administrative fine shall be imposed on that person, the amount of which may not be less than ten thousand euros (€ 10,000) and more than five hundred thousand euros (€ 500,000). In assessing

the above penalty, account shall be taken in particular of the gravity of the infringement and the degree of fault.

10. False Reporting & Protection against False Reporting

The Group will protect those who file a Report in good faith. However, it reserves the right to take action against any person or vendor involved, if it is proven that s/he intentionally or fraudulently provided false information when filing a Report. A Reported Person who directly or indirectly suffers prejudice as a consequence of a Report made in bad faith, shall retain the protection and the remedies available to him/her under the applicable legislation. In any case, the Reported Person shall have the right to express his/her views in a manner that does not jeopardize the conducted investigation.

Especially with respect to Reports of Group A Violations, persons who ***knowingly*** proceed in false reporting or public disclosures shall face sanctions, including penalty of imprisonment (of at least 2 years) and monetary fines. Reports are considered to have been submitted in bad faith, if they are filed maliciously, with reckless disregard for their truth or falsity and/or for the sole purpose of harming the Group, the Reported Party/-ies or other persons. Employees filing such a Report in bad faith may be subject to disciplinary measures or other legal measures at the discretion the Group.

11. Revision History

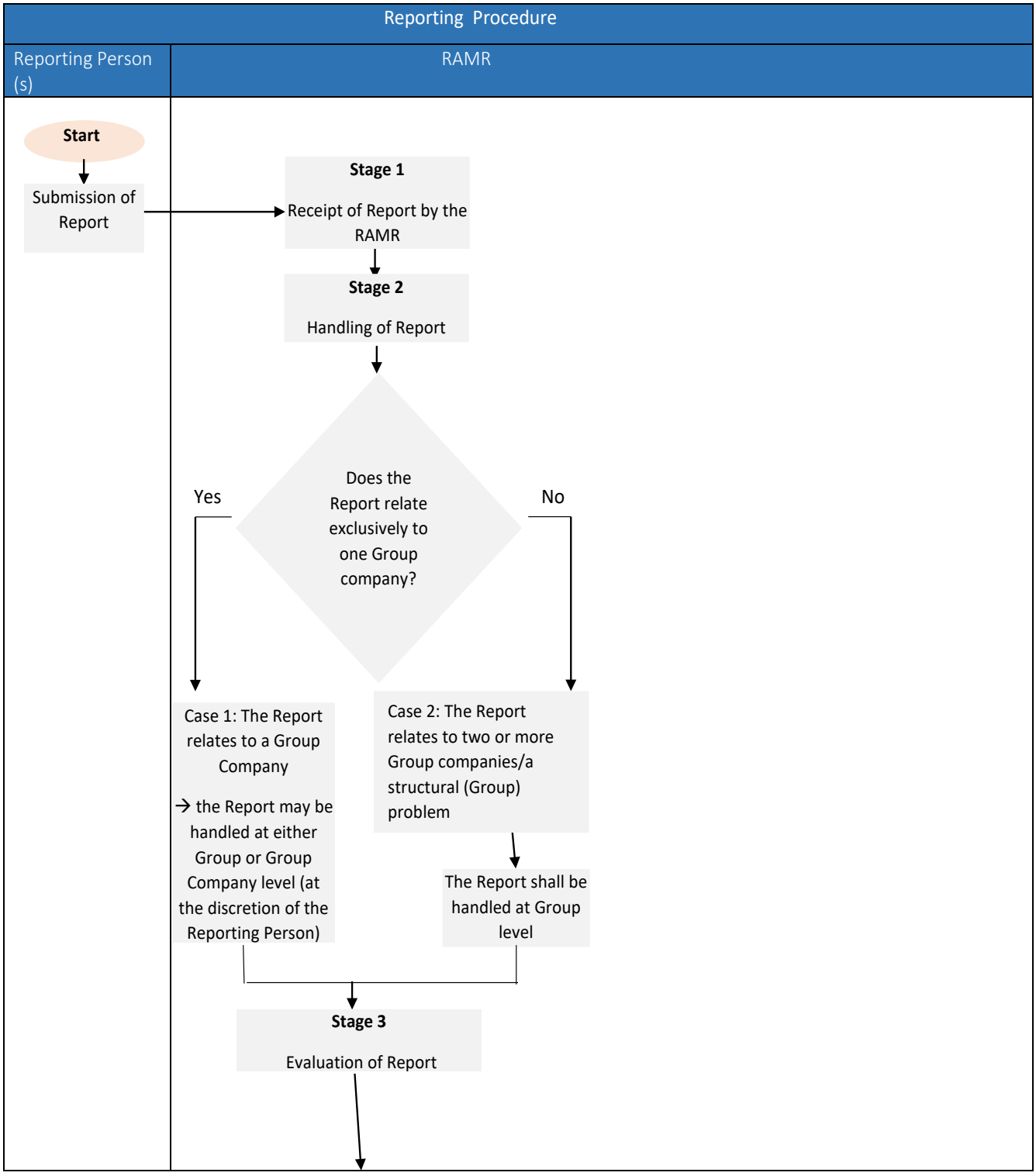
Version	Date	Owner	Comments / Main Changes
1	10/05/2023	K. Giannakakou-Razelou	1st version for implementation

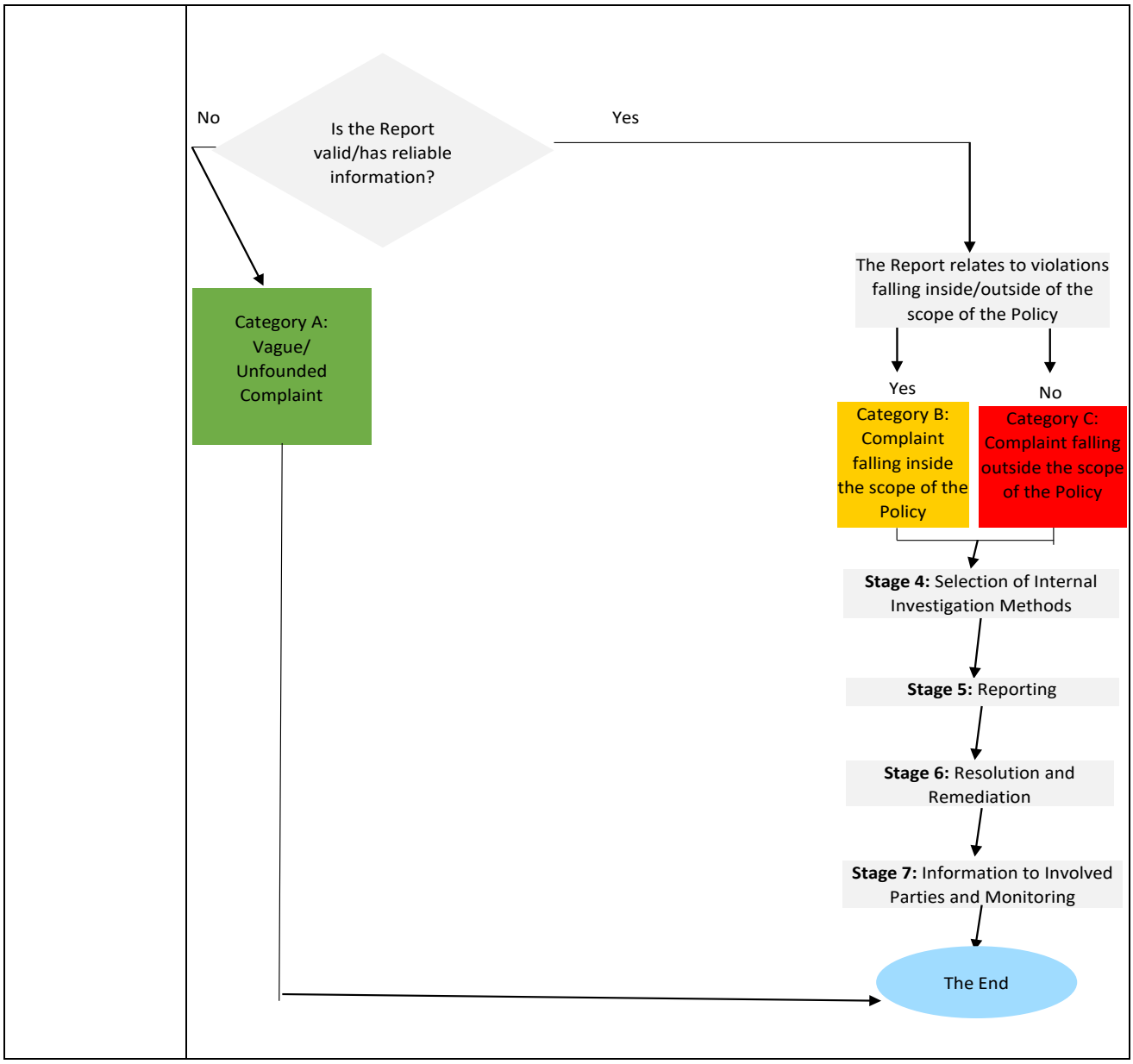
12. Document Approvals

	Name	Position
Owner	K. Giannakakou-Razelou	Legal Manager – RG & Corporate Compliance
Reviewed & Approved	G. Koumantakis	Legal Director – Corporate & Network Compliance
Approved	V. Vasilopoulou	Legal Director – Corporate & Commercial Affairs
Approved	N. Verra	Chief Legal, Regulatory & Compliance Officer
Approved	BoD Resolution 4 /27.04.2023 (Item 2)	

Annex 1 - Whistleblowing Procedure

1. Flowchart




No
Is the Report valid/has reliable information?
Yes
Category A: Vague/ Unfounded Complaint
The Report relates to violations falling inside/outside of the scope of the Policy
Yes
No
Category B: Complaint falling inside the scope of the Policy
Category C: Complaint falling outside the scope of the Policy
Stage 4: Selection of Internal Investigation Methods
Stage 5: Reporting
Stage 6: Resolution and Remediation
Stage 7: Information to Involved Parties and Monitoring
The End

2. Detailed Procedure

A. Receipt of report

The following internal Reporting Channels may be used for the submission of a Report by the Reporting Person(s).

Reports may be:

a. submitted via the reporting platform, which can be accessed via the Company's intranet and website (e-platform),

b. sent to the e-mail address whistleblowing@opap.gr (or dedicated e-mail address of a Group Company, if available)

c. sent by post to the Group Companies' address, marked as "Confidential", and to the attention of the RAMR,

d. submitted directly to the RAMR, orally or in written form.

The above communication networks operate as internal Reporting Channels. Channels under a and b are available all days and hours during the week. Any expression of complaint, dissatisfaction, opinion and/or grievance, which is not submitted in compliance with the established procedure may not be treated as a Report by the Group Companies.

The RAMR is responsible for receiving Reports and informing the competent employees or executives with respect to the Report in scope. In case the Report is submitted through the e-platform, the Reporting Person is notified about the receipt of the Report immediately and in any case, with respect to Reports for Group A Violations within seven (7) days as of such receipt.

In case a Report has not been received through the e-platform, but through any other Reporting Channel, the RAMR shall register it in the Reports registry and shall also notify the Reporting Person of the receipt as soon as possible and, in the case of Reports for Group A Violations, within seven (7) days of such receipt.

B. Handling of reports

The RAMR is the recipient of the Reports and is responsible for initiating the internal investigation of any Report identified thereunder, in accordance with applicable policies and processes.

The RAMR shall direct and oversee the investigation of the Reports and engage with the competent person(s) s/he determines to be appropriate for each case, and, if necessary, shall delegate the Report's oversight and investigation to the competent person(s) of the Group Company involved. Depending on the nature of the reported violation, the RAMR shall engage with the Chief Financial Officer, the Chief Legal, Regulatory and Compliance Officer, the Chief People Officer, the Data Protection Officer, the AML Officer, the Head of the Internal Audit, executives from Group Companies, the Audit Committee, the Board of Directors or outside advisors, as appropriate, provided that, to the extent known, the identity of the Reporting Person is kept undisclosed to the relevant delegated entity, person or outside advisor.

Depending on the Group Company/-ies affected or involved in a reported incident, the Report shall be handled at Group Company level or by OPAP S.A. RAMR as provided in Section 6.2.A (for

Reports revealing a structural problem or a problem affecting two or more Group Companies). If the Report involves members of the Board of Directors, it is handled exclusively by the RAMR in cooperation with executive BoD Members not affected by the Report.

In any case, deadlines set by the applicable framework, including the relevant framework for the processing of personal data, shall be respected, with emphasis on the obligation to notify the Reporting Person about the status of his/her Report within three (3) months from its submission, with respect to Reports for Group A Violations. Regarding Group B violations, the Reporting Person shall receive an update on the status of his/her Report within six (6) months from its submission.

C. Evaluation of report

Immediately after receipt of the Report, the RAMR shall carry out a core assessment of the Report, examining the credibility and validity thereof, in order to categorize it accordingly between the following categories A, B or C.

Category A: Vague/unfounded Report

Where the Report is: a) incomprehensible, or b) not sufficiently justified, or c) clearly unfounded due to unreliable information, or d) submitted in an abusive manner, the RAMR may decide that no further investigation is required and archive the Report.

Category B: Reports of breaches falling inside the scope of the Policy

If the Report refers to violations falling inside the scope of this Policy, and problems, inappropriate conduct, or breaches of the applicable framework are identified, then corrective steps must be taken. The handling of the Report and its further investigation is assigned to the RAMR, who shall engage with the competent person(s), Unit(s), Group Company/-ies or escalate it accordingly. The RAMR may engage with the Internal Audit, the Audit Committee of the Board of Directors as deemed necessary for the effective handling of the Report. The RAMR shall indicate whether a Report concerns Group A or Group B Violations and handle it accordingly, taking into consideration the special framework and protection measures applicable for Group A Violations.

Category C: Reports falling outside of the scope of the Policy

If the Report relates to other breaches that fall outside the scope of this Policy, (*e.g.,* harassment, use of force/violence, unethical workplace behavior, insult, etc.), the handling of the Report and its further investigation is assigned to People Team and/or Legal, Regulatory and Compliance Team, in cooperation with the relevant business units.

D. Selection of internal investigation methods

Depending on the classification category (B or C) and in cooperation with the competent person(s)/Unit(s), the RAMR shall take the following actions, if necessary:

First, the scope and type of the investigation is determined. Indicatively and in accordance with each Group Company's individual policies (where applicable), i) interviews may be conducted to gather evidence/probative value; ii) an autopsy and/or on-site inspection may be carried out at the Group Company's premises; iii) special consultants may be engaged (experts, psychologists, economists, legal advisors and IT companies, etc.); iv) an audit on the company's IT resources may be carried out.

Crucial to the use of the evidence gathered through the investigation is the lawfulness of the process and the safeguarding of the rights of the parties involved. Therefore, and if necessary, the relevant person(s)/Unit(s) shall consult with the RAMR and the Data Protection Officer prior to the implementation of the action plan and obtain an opinion on the legality and scope of the intended internal investigations.

E. Reporting

Upon completion of the action plan, the RAMR prepares the investigation/evaluation report with his/her findings. The RAMR periodically informs the Board of Directors and/or the Audit Committee with respect to the Reports received and their progress and shall *ad hoc* inform the Board of Directors in case of an emergency or in case of a serious violation.

Upstream knowledge sharing

For knowledge sharing purposes, the Group Companies shall submit to the RAMR and Deputy RAMR of OPAP S.A. an annual report on the Reports filed through their designated internal channels, stating also the remedial actions taken. Confidentiality legal requirements will always be respected.

F. Resolution and remediation

At this stage, the competent person(s)/Unit(s) implements measures to address and remediate the incident, if feasible.

Furthermore, the competent person(s)/Unit(s) in collaboration with the RAMR, shall examine the obligation to notify the supervisory authorities.

At the same time, if the Board of Directors wishes to take a judicial recourse against the parties involved to defend the Group's legitimate interests, the Chief Legal, Regulatory and Compliance Officer shall support the Board of Directors in deciding if the procedure will be initiated.

Finally, the competent person(s)/Unit(s) shall take appropriate measures to ensure, if possible, that the cause of the Report is eliminated.

G. Informing involved parties and monitoring

In collaboration with the competent person(s)/Unit(s) (if required), the RAMR and/or the Data Protection Officer, shall examine the obligation to notify the Reporting Person, the Reported Party or any other parties involved.

When a case follows the judicial course, the Chief Legal, Regulatory and Compliance Officer shall monitor the progress and shall maintain communication with both the Reporting Person and the Reported Party, if necessary.

In cooperation with the person(s)/Unit(s) involved in each case, the RAMR shall make recommendations for obtaining the necessary measures to avoid similar incidents in the future.

3. Steps Description

A/N	Responsible Party	Activity / Action Description
1	Reporting Person	**Submission of Report** Submission of Report for an irregularity, omission, or misconduct through any of the following internal Reporting Channels: • E-platform, • Company's e-mail address, • mail to the Company's address, marked as "Confidential" and to the attention of the RAMR, • written or verbal communication directly with the RAMR.
2	RAMR	**Stage One: Receipt of the Report** The RAMR receives the Report and engages with the competent person(s)/Unit(s). In case the Report has not been submitted via the e-platform, the RAMR shall notify the competent person(s) and manually register the Report in the e-platform.
3	RAMR	**Stage Two: Handling of the Report** The RAMR conducts an initial assessment, reviewing the key elements of the Report in order to clarify the Group Company to which it relates.
4	RAMR	**Stage Three: Evaluation of the Report** The RAMR, in cooperation with the competent person(s)/Unit(s), conducts a further assessment, examining the credibility and validity of the Report, in order to categorize it into categories A, B or C (as described below), as appropriate. The assessment is filed on the e-platform to ensure confidentiality. The obligation/time to inform the Reporting Person and other involved persons is evaluated and a resolution action plan is delimited.
5	RAMR	**Vague Report** Where the Report is a) incomprehensible, or b) not sufficiently justified, or c) clearly unfounded due to unreliable information, or d) submitted in an abusive manner, the RAMR may decide that no further investigation is required. The assessment is filed on the e-platform, with appropriate commentary. The Report is archived. *Completion of the Process.*

A/N	Responsible Party	Activity / Action Description
6	RAMR in cooperation with competent person(s)/Unit(s)	**Report concerns breaches falling in the scope of the Policy** If the Report refers to violations falling inside the scope of this Policy, and problems or inappropriate conduct or breaches of applicable framework are identified, corrective steps must be taken. The handling of the Report and its further investigation is assigned to the RAMR, who shall engage with the competent person(s), Unit(s), Group Company/-ies or escalate it accordingly. The flowchart continues on stage 4.
7	RAMR People Team Legal Regulatory and Compliance Team	**Report concerns breaches falling out of the scope of the Policy** If the Report relates to other breaches that fall outside the scope of this Policy, (*e.g.,* harassment, use of force/violence, unethical workplace behavior, insult, etc.), the handling of the Report and its further investigation is assigned to the People Team and/or the Legal, Regulatory and Compliance Team, in cooperation with the relevant business units.
8	RAMR Legal, Regulatory and Compliance Team DPO Competent person(s)/Unit(s)	**Stage Four: Selection of Internal Investigation Methods** Depending on the classification category (B or C) and in cooperation with the competent person(s)/Unit(s), the RAMR shall take the following actions, if necessary: • Examine the necessity to involve external partners for resolution (if necessary, contact an external partner) • Select the appropriate investigative measures (*e.g.,* interviews with the parties involved, collection of evidence, etc.). • Establish a working group for the investigation. • Request an opinion from the DPO on the legality and scope of the intended internal investigations, before the beginning of the investigation procedure.
9	RAMR	**Stage Five: Reporting** Investigation/evaluation report with findings/resolution. Notify the Board of Directors.
10	RAMR in cooperation with competent	**Stage Six: Resolution and Remediation** • Submit resolution proposals, if feasible. • Explore further legal action, if necessary.

A/N	Responsible Party	Activity / Action Description
	persons/Units	• Inform the relevant Supervisory Authority, if necessary.
11	RAMR Involved persons/Unit(s)	**Stage Seven: Informing Involved Parties and Monitoring** • Investigate if and how the Reporting Person and the Reported Party were notified through the e-platform. • If further legal actions take place, the RAMR monitors their progress. • The RAMR maintains communication with the Reporting Person and the Reported Party, if necessary. • The involved person(s)/Unit(s) shall make recommendations aiming to avoid similar incidents in the future by taking the necessary measures.