FAIS HOLDING SOCIETE ANONYME

(distinctive title: FAIS GROUP S.A.)

POLICY ON THE REPORTING OF MISCONDUCT

(Whistleblowing Policy)

Scope of application: FAIS HOLDING SOCIETE ANONYME
Tax Reg. No.: 800907275
G.E.MI. No.: 144651701000
Date: 12 December 2023
Version: 1.0
Level of effect: Binding

COURTESY TRANSLATION

This is an unofficial English-language translation of the Greek original. In case of any discrepancy between the Greek original and this English translation, the Greek version shall prevail.

Table of Contents

1. Introduction 3
2. Definitions 4
3. Objectives of the Policy 5
4. Scope of Application 5-6
5. Types of Misconduct 7-8
6. Responsibilities of the RMRO 8-9
7. Procedure for the Submission and Handling of Reports 9-11
8. Corrective Actions & Disciplinary Sanctions 11
9. Anonymity – Confidentiality 11
10. Protection of Personal Data 12
11. Management Commitments 12
12. Retaliation & Protection from Acts of Retaliation 12-13
13. Information about this Policy 13

1. Introduction

The company FAIS HOLDING SOCIETE ANONYME, across the entire range of its activities, undertakes to operate in accordance with the rules of ethics and the applicable legislative and regulatory framework, with the aim of creating sustainable value, pursuing the maintenance of high standards of corporate governance, transparency, as well as professional and ethical conduct. For this reason, it demonstrates zero tolerance for actions that may disrupt the healthy working environment, harm it, and expose its reputation and reliability to risk.

The cultivation and establishment of a stable, modern and healthy corporate environment that promotes the work of FAIS HOLDING SOCIETE ANONYME and is characterised by the principles of integrity, honesty and regulatory compliance, is an obligation of all, and a fundamental prerequisite for healthy business activity and social cohesion and progress. FAIS HOLDING SOCIETE ANONYME undertakes to conduct its business activities with honesty and integrity, and expects everyone, irrespective of their relationship with the company, to maintain a high standard of ethical conduct and to comply with the laws, corporate policies and procedures.

In the context of sound corporate governance and regulatory compliance, FAIS HOLDING SOCIETE ANONYME (the "Company") has developed a Whistleblowing Policy (the "Policy"). The Policy is adapted to the principles and provisions of European Directive 2019/1937 on the protection of persons who report breaches, which was incorporated into the national legal order by Law 4990/2022, as well as the international best practices that have been developed for internal reporting. The purpose of this Policy is (a) the compliance of the Company with the (EU) Directive, and (b) to set out the principles and the relevant framework within the Company.

The Company encourages all those referred to in paragraph 4 of article 5 to report, confidentially or anonymously, through the existing Reporting channels, conduct that is unlawful and/or unethical, immediately upon coming to their knowledge.

Whistleblowing means the voluntary act of disclosure by any person who is aware either of misconduct, significant irregularities and omissions, or of other unethical and unlawful acts that have already been committed, or in respect of which there is an indication and intention of possible commission within the Company.

In the context of this Policy, the employees of the Company and/or third parties are encouraged and urged to report, on a named or anonymous basis, serious and genuine reports of misconduct, irregularities, omissions or punishable acts that have come to their knowledge. The same applies to any concerns, anxieties or complaints on matters relating to the breach of the policies of the Company and/or of the law.

2. Definitions

1. "Report": The oral or written provision of information regarding breaches in the Company.

2. "Person Concerned": a natural or legal person who is named in the report as the person to whom the breach is attributed, or who is connected with the person to whom the breach attributed under the scope of this Policy is ascribed.
3. "Reporting Person": the person who reports or discloses information regarding breaches obtained in the context of their work or cooperation with the Company.
4. "Retaliation": any direct or indirect act or omission that occurs within the working context, causes or is likely to cause unjustified harm to the Reporting Person, or to place them at a disadvantage, and is connected with a report.
5. "External Associates": Third parties connected, contractually or otherwise, with the Company, as well as their personnel, specifically consultants, subcontractors, contractors, suppliers, shopkeepers of commercial centres, associates of any nature, shareholders, etc.
6. "Officer for the Receipt and Monitoring of Reports" or "RMRO": the person competent for the handling and investigation of reports.
7. "Employee": the person with a fixed-term or indefinite-term employment contract, or the person connected with the Group by another employment relationship, or the person who constitutes seasonal personnel, or the person engaged as a trainee of a company of the Group.
8. "Reporting Channels": the means through which Reports are submitted and which include the means used for the submission of reports, as well as the persons to whom the Reporting Persons may address themselves.
9. Malicious Report: the Report made by the Reporting Person with knowledge that it is not true.
10. Good faith: The state which gives rise in the Reporting Person to a reasonable belief that they validly consider the information they provide to be true.
11. Personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, as well as the processing of genetic data, biometric data for the purposes of uniquely identifying a person, data concerning health, or data concerning the sexual life or sexual orientation of a natural person.
12. Confidentiality of identity: in cases where the report is on a named basis, the identity of the Reporting Person must be kept secret from the Officer for the Receipt and Monitoring of Reports and from the person who may be involved in the report/complaint.
13. Anonymity: the state in which the identity of the person filing the report, concern or complaint is not made known.

3. Objectives of the Policy

The objectives of this Policy aim at:

- Encouraging the disclosure of any unlawful act, irregularity, improper, inappropriate or unethical conduct.
- Clarifying the reporting procedure and its handling.

- Preventing or deterring misconduct that could otherwise cause financial loss to the Company or harm its reputation.
- Assuring that all reports will be treated with absolute discretion, seriousness and diligence, without negative consequences (retaliation) of any form against the person who has made the report.
- Cultivating and developing a culture of accountability, compliance and integrity.
- Assuring employees of support when they submit reports where they identify or suspect improper, unethical or inappropriate conduct in the Company.

The fundamental and inviolable objective of the Policy is the protection of the anonymity and confidentiality of the data of the persons who submit such reports. Furthermore, where they are employees of the Company, the assurance that their future development is not endangered. In the event of a named complaint, it is assured that there will be no consequences for the person submitting the complaint.

4. Scope of Application

This Policy applies to the protection of persons who report or disclose:

14. Breaches of acts of the rules of EU law, as more specifically set out in Part I of the Annex to Law 4990/2022 (Annex I of this Policy), as well as acts that may subsequently be issued thereunder as secondary acts, in the fields of:

- Public procurement;
- Financial services, products and markets, as well as the prevention of money laundering and terrorism financing;
- Product safety and compliance;
- Transport safety;
- Protection of the environment;
- Radiation protection and nuclear safety;
- Food and feed safety, as well as animal health and welfare;
- Public health;
- Consumer protection;
- Protection of privacy and personal data, as well as the security of network information systems.

15. Breaches affecting the financial interests of the Union under article 325 of the Treaty on the Functioning of the European Union (TFEU), namely cases of fraud or any other unlawful activity against the financial interests of the EU, and as more specifically set out in the relevant Union measures.

16. Breaches related to the internal market, namely the area of the EU within which the free movement of goods, persons, services and capital is ensured, as referred to in paragraph 2 of article 26 of the TFEU, including breaches of the rules of the Union on competition and State aid, as well as breaches concerning the internal market in relation to acts that contravene the rules on corporate taxation, or arrangements the purpose of

which is to ensure a tax advantage that defeats the object or purpose of the applicable corporate-taxation legislation.

17. The Policy applies and has effect in all organisational structures of the Company, and is addressed to and concerns any person who works, provides services, cooperates with the Company, and any third party connected with the Company, specifically:

- Employees on full-time or part-time, permanent or seasonal employment;
- Non-salaried persons, self-employed persons, consultants, or home-based workers;
- Shareholders and persons belonging to the administrative, management or supervisory body, including non-executive members, as well as volunteers and trainees, whether paid or not;
- Employees of contractors, subcontractors and suppliers; and
- Former employees (including pensioners) and candidate employees.

5. Types of Misconduct

A. Categories falling within the raising of concerns – Reports

The types of misconduct, in the broader sense, are understood as unlawful, irregular, dangerous or unethical acts carried out in the context of the activities of the Company and which give rise to issues of liability.

Examples of such conduct/acts are listed below indicatively. The list below should not be considered exhaustive or restrictive.

- Breach of Union and national law (laws, European directives, etc.);
- Harm or threat to the public interest (public health and safety, environment, money laundering, fraud and corruption issues in public procurement, etc.);
- Leakage of confidential information;
- Harm or threat to the corporate interest;
- Theft, embezzlement;
- Fraud;
- Forgery;
- Defamation;
- Money laundering from criminal activities;
- Conflict of interest;
- Bribery;
- Intimidation;
- Discriminatory treatment;
- Abuse of authority / corruption;
- Harassment of any kind;
- Waste of corporate resources;

- Abuse of assets;
- Breach of corporate / professional secrecy;
- Breach of the legislation and policy of the Company on the protection of personal data, as well as on privacy;
- Breach of corporate governance principles regarding the concealment of, or failure to identify, conflict-of-interest situations;
- Falsification of financial statements or provision of falsified financial information;
- Consumer protection issues;
- Any breach of the Code of Ethics and Conduct;
- Breach of the law, and by extension of the corporate policy, on the prevention and combating of violence and harassment;
- Tolerance of reprehensible conduct;
- Concealment or covering up of any of the above.

B. Categories which do not concern the system for raising of concerns, in accordance with the Policy

The following reports, where it is established that they relate to such matters, are not investigated further (the list is indicative):

- Information that has already been made public;
- Rumours and gossip without substantiated evidence;
- Trivial matters;
- Disagreements that do not breach laws or do not constitute ethically inappropriate conduct;
- Cases of handling of customer complaints that fall within the usual operation of the Company and which are handled by the internal mechanism;
- Cases relating to personal disputes and disagreements on personal matters and personalities.

6. Appointment / Responsibilities / Duties of the RMRO

Appointment:

The Head of Human Resources has been appointed in the capacity of the Officer for the Receipt and Monitoring of Reports (RMRO).

Responsibilities:

The RMRO has the following responsibilities:

- To provide the appropriate information regarding the possibility of submitting a report within the Company, and to disseminate the relevant information at a visible location of the Company;
- To receive reports regarding breaches falling within the scope of this Policy;

- To confirm the receipt of the report to the Reporting Person;
- To carry out the necessary actions in order for the competent body / assessment committee of the Company to take up the report, or to conclude the procedure by filing the report;
- To ensure the protection of the confidentiality of the identity of the Reporting Person and of any third party named in the report, by preventing access to it by unauthorised persons;
- To monitor the reports and maintain communication with the Reporting Person and, where required, to request further information from them;
- To provide information to the Reporting Person on the actions taken;
- To provide clear and easily accessible information regarding the procedures under which reports may be submitted to the National Transparency Authority and, as the case may be, to public bodies or to institutional and other organs or bodies of the European Union; and
- To design and coordinate training actions regarding ethics and integrity, and to participate in the development of internal policies for the enhancement of the integrity and transparency of the Company.

Duties:

The RMRO must:

18. Exercise their duties with integrity, objectivity, impartiality, transparency and social responsibility.
19. Respect and observe the rules of discretion and confidentiality on matters of which they have become aware in the exercise of their duties.
20. Refrain from the handling of specific cases by declaring an impediment, where a case of conflict of interest arises.

7. Procedure for the Submission and Handling of Reports

7.1 The Company has established multiple, easily accessible and available channels of reports/complaints which permit the submission of a report in writing (by post, email) or orally. Specifically, it encourages the sending of reports/complaints through the following communication channels:

(a) orally by telephone (2111 088 551) or by personal meeting with the RMRO within a reasonable period, upon request of the Reporting Person;

(b) in writing by sending an electronic mail message to the address (whistleblowing@faisgroup.gr);

(c) in writing, on a named or anonymous basis, by sending a postal letter to the RMRO of the Company (Poseidonos Avenue 77, Alimos 174 55, 4th floor).

In the case of submission of a report by telephone, where the call is not recorded, the RMRO must draw up minutes of the conversation, providing the Reporting Person with the opportunity

to verify, correct and/or supplement and agree with the minutes of the conversation by signing them.

Where a person requests a meeting with the RMRO in order to submit the report in person, full and accurate minutes of the meeting drawn up by the RMRO are kept, providing the interested party with the opportunity to verify, correct and/or supplement and agree with the minutes of the meeting by signing them.

In the event of refusal to sign the minutes provided for above, a relevant note is made on the minutes by the RMRO.

7.2 Upon submission of any report, the following handling and investigation procedure will be followed:

The RMRO:

- Confirms the receipt of the report to the Reporting Person promptly and in any event within seven (7) business days from the day of receipt;
- Maintains a Central Register of Reports;
- Takes every appropriate measure for the protection of the personal data of the data subjects involved in the Reports and sees to their deletion in accordance with the prescribed periods;
- Assesses and prioritises the Reports;
- Convenes a meeting with the Report Assessment Committee, composed of the Chief Financial Officer, the Data Protection Officer and the Payroll Officer, for the processing of the report(s).

7.3 The Officer for the Handling of Reports, where required, conducts an investigation of the facts contained in the Report. Where deemed necessary and depending on the subject matter of the Report, they may receive additional professional support from other executive officers of the Company, as well as from external consultants.

7.4 The RMRO provides information to the Reporting Person on the actions taken within a reasonable period of time, which shall not exceed three (3) months from the expiry of seven (7) days from the submission of the report.

7.5 In the event of rejection of the report, the procedure is concluded, the RMRO files the report and notifies the Reporting Person in writing of the decision, including the reasons for the rejection.

The reasons for rejection may relate to cases where:

- The reported acts do not fall within the scope of application of this Policy;
- The report is unintelligible or is submitted abusively, or does not contain facts that substantiate a breach of Union law, or there are no serious indications of such a breach;
- It has been established that the report was not made in good faith.

7.6 Rights of those named in the Reports

- The persons named in the Reports have the right to be informed promptly of the misconduct of which they are accused, of the persons who have access to the data

contained in the Report or in the report, and of the right to be called to provide an explanation.

7.7 Lack of satisfaction with the outcome of the investigation of the report

- If the Reporting Person considers that their internal Report was not addressed effectively, they may resubmit it to the National Transparency Authority (NTA). The instructions are set out on their relevant website www.aead.gr.

8. Corrective Actions and Disciplinary Sanctions

Depending on the results of the investigation, the Officer for the Handling of Reports proposes corrective actions and/or disciplinary sanctions, depending on the degree of severity. The actions/sanctions may include:

21. Additional training of employees;
22. Creation and implementation of new internal control safeguards;
23. Amendments to existing procedures and policies;
24. Disciplinary sanctions which may include up to dismissal;
25. Judicial actions.

9. Confidentiality – Anonymity

- Personal data and any kind of information that leads to the identification of a person, directly or indirectly, are not disclosed to anyone other than the authorised members of personnel competent to receive or monitor the reports.
- By way of derogation from the above, the identity of the Reporting Person and any other information may only be disclosed in cases where this is required by Union or national law, in the context of administrative, civil or criminal investigations of the competent public authorities, or in the context of judicial proceedings, and provided that this is necessary for the service of the purposes of Union or national law, or for the safeguarding of the rights of defence of the Person Concerned.
- Disclosures pursuant to the preceding paragraph of this chapter are made after the Reporting Person has been informed in writing of the reasons for the disclosure of their identity and of other confidential information, unless such information would undermine the investigations or judicial proceedings. Following the information, the Reporting Person is entitled to submit observations in writing to the Company making the disclosure pursuant to paragraph 2, which are not disclosed to anyone. Exceptionally, where the grounds put forward in the observations are not deemed sufficient, the disclosure of the identity and other confidential information of the Reporting Person is not impeded. Further safeguards of the identity of the Reporting Person and of the information from which such identity may be inferred, provided by special provisions of Union or national law, are not affected.

10. Protection of Personal Data

- Any processing of personal data hereunder is carried out in accordance with Regulation (EU) 2016/679 and the relevant provisions of national and European legislation on the protection of personal data, as in force, as well as the policies and regulations on personal-data protection of the Company, which are published on the internal intranet https://faisgroupnews.gr/. The data of all those involved are protected and are processed exclusively in relation to each Report and with the sole purpose of ascertaining the substantiation or otherwise of the Report and of investigating the specific incident.
- The Company takes all necessary technical and organisational measures for the security of personal data and their protection, in accordance with the above.
- Sensitive personal data and other data not directly related to the Report are not taken into account and are deleted.
- Access to the data contained in the Reports may be had only by those involved in the handling and investigation of the incident, such as, for example, the members of the Report Assessment Committee and the Officer for the Handling of Reports, including specialised external consultants.
- The personal data are deleted from the Register of Reports within a reasonable period of time following the conclusion of the investigation initiated on the basis of the Report.

11. Management Commitments

Reports are treated by Management as a legitimate act which may contribute to the efficiency and smooth operation of the Company, and are accordingly encouraged.

Management acknowledges that such a system of internal disclosure of improper practices, without fear of retaliation, indicates that employees take their responsibilities seriously and contribute to the avoidance of the negative publicity that usually follows such disclosures to external bodies.

Management is accordingly committed to cultivating a culture of accountability, integrity and regulatory compliance with zero tolerance for any harassment, victimisation or discrimination of the Person Concerned, provided that the Report is made in good faith and is not based on rumours and speculation.

12. Retaliation – Protection from Acts of Retaliation

Definition and forms of retaliation

Retaliation means any actions originating from anyone (members of management, supervisors of the person filing a Report, colleagues, associates, external consultants, suppliers, customers) who may cause, directly or indirectly, adverse situations to the Reporting Person.

The definition of retaliation includes, but is not limited to, the following:

- Dismissal;
- Non-renewal or early termination of a fixed-term contract;
- Discontinuation of acceptance of services;

- Non-provision of a letter of recommendation;
- Damage to reputation;
- Unjustified negative assessment of performance;
- Restriction of the duties and responsibilities included in the job description;
- Workplace harassment (mobbing) in any manner and by any means;
- Adverse and unilateral detrimental changes to the terms of the employment contract;
- Hindering the exercise of employment rights, such as, for example, the non-granting of leave, participation in training programmes, etc.

In such a case, the person who suffered such retaliation may file an official report with the Report Assessment Committee, which is required to inform the Board of Directors and to request, by every means, protection from the Company (practical and legal support, advisory support, transfer to another service, etc.) in order to be protected from possible adverse reactions in the working environment.

13. Information about this Policy

The Officer for the Handling of Reports ensures that all employees of the Group are expressly informed about the content of this Policy. The information is provided through the dispatch of informative material, email, the internal intranet, or by any other appropriate means depending on the access of the employees.