Speak Up Policy

Version Control			
Date	**Version**	**Approver**	**Notes**
15/07/2021	1.0	BoD	Initial Approval
05/05/2025	2.0	BoD	Update

Contents

1. Introduction

GR. SARANTIS SA (Address: 26, Amaroussiou - Halandriou Street, 151 25 Maroussi, Athens, Greece, Tel: +30 210 6173000, Fax: +30 210 6197081, e-mail: gr-info@sarantisgroup.com, website: https://greece.sarantisgroup.com/ (hereinafter, "**Sarantis**" or the "**Company**") and its worldwide Affiliates (hereinafter, collectively referred to as the "**SARANTIS Group**" or the "**Group**") sets as a priority its activity within a framework governed by the highest level of ethics and professional conduct. For this reason, it ensures that its Board of Directors as well as the management team and its employees, comply with legal and/or regulatory requirements applicable in the territories in which SARANTIS Group operates, as well as relevant internal policies and procedures established by the Company and that their actions are characterized by honesty, integrity, and high moral values.

In this context and in order to ensure the integrity and effectiveness of the corporate culture, and the ethics and reliability promoted by the Company, SARANTIS Group has established this Speak Up Policy (hereinafter, the "**Policy**") intended to outline the conditions for ethical reporting and handling of related reports across the SARANTIS Group.

The Policy defines the principles and the organizational model adopted by the Company to receive, process and investigate eponymous and/or anonymous reports and complaints regarding unethical behaviours, irregularities, omissions or criminal acts. This Policy applies to all Group entities and their personnel.

By this Policy the Company undertakes to safeguard the protection of anonymity and to guarantee the confidentiality of the personal data of the persons who submit such reports/complaints.

The Policy ensures compliance with the provisions of the Whistleblowing Directive (EU) 2019/1937, along with the relevant implementing laws and national legislation of both EU and non-EU countries, where SARANTIS Group operates, as well as best practices adopted in the relevant territories.

Policy purpose

1.1. The purpose of this Policy is to set out the conditions for the internal management of reports and complaints concerning the violation of legal provisions, regulations, internal policies and procedures of the Company, and in particular any non-compliance with the Company's Code of Ethics, or with the performance of any act or omission which could damage the reputation, activities and assets, executives and staff of the Company. The mechanism for submitting, investigating, and evaluating reports and complaints as well as all the individual elements described in the Policy have been established to effectively manage the submitted reports and complaints, providing adequate and appropriate guarantees to ensure the protection of personal data and privacy, on the other hand, the protection against malicious reports and complaints which are not based on facts.

1.2. In case of a personal complaint, the Company takes all necessary measures and assures that there shall be no negative consequences, in the form of retaliation, to the detriment of the person filing the complaint. As a negative consequence, in the form of retaliation, is defined any positive or negative action and/or omission which aims at the professional demotion and/or personal devaluation of the person who submitted the report/complaint.

2. Definitions

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/Whistleblower	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.
Whistleblowing Officer	Responsible person for the acceptance and monitoring of Reports.
Whistleblowing Committee	A body composed by the Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Human Resources Officer (CHRO), Whistleblowing Officer, Group Legal Counsel and on a case-by-case basis, the local General Manager.
Breaches	Actual or suspected irregular, illegal, unfair, unethical, or criminal acts or omissions falling within the scope of this Policy.
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).
Good Faith	The Reporting Person's reasonable belief that their Report is truthful, based on objective facts and circumstances.
Retaliation	Any direct or indirect act or omission, occurring within the work-related context, which causes or is likely to cause undue prejudice to the Reporting Person or persons associated with them, or to put the Reporting Person or persons associated with him at a disadvantage and connected with the Report.

3. Who can make a Report?

3.1. This Policy applies to the following categories of individuals (hereinafter, the "**Reporting Persons**") submitting a whistleblowing report (hereinafter, the "**Report**").

3.2. Reporting 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 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.

3.3. Persons (of any of the capacities referred to above under Section 3.1), who acquired information on a breach of law in a work-based relationship which has since ended.

3.4. Persons (of any of the capacities referred to above under Section 3.1), whose work-based relationship is yet to begin, where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

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

The Reporting Person is protected on the condition that they act in good faith and that they have reasonable grounds to believe that the information they provide in the relevant Report is true and accurate and falls within this Policy's scope of application.

4. What type of misconduct can be reported?

4.1. Any individual subject to this Policy who becomes aware of misconduct within the Group must promptly report the matter through the designated Reporting Channel(s).

4.2. The list below is not exhaustive but serves to illustrate the types of misconduct covered under this Policy, typically associated with one or more of the following breaches:

- acts related to money laundering, terrorist financing;
- acts involving evidence of gross negligence, suspected fraud or corruption;
- bribing (offering or accepting bribes);
- theft, embezzlement, forgery, misuse of any Group company's assets;
- infringements of intellectual and industrial property rights;
- violations of free and fair competition law;
- acts that affect the purpose and reputation of any Group company;
- operations conflict with the interests of the Company, or acts that violate the rules of ethics that govern the activity and internal organization of any Group company;

- acts that violate personal data, whether related to employees, customers, suppliers, partners, or others, as well as privacy and confidentiality breaches;
- acts that violate the policies and procedures established by the Company, including inappropriate behaviour, intimidation, abuse of power, sexual harassment etc.;
- operations that endanger the health and safety of employees and customers of any Group company;
- acts harmful to the environment;
- irregularities or misconduct related to public procurement.

4.3. The following types of Reports are out of scope of this Policy:

a) reports concerning violence and sexual harassment in the workplace affiliated with Greece and/or Poland;
b) disputes over employment or personal matters between colleagues or employees and superiors or policies and decisions of the Company's Management;
c) customer disputes with the Company in the context of their commercial cooperation,
d) consumer reports and complaints regarding the quality of services and products provided by the Company.

In case a Report concerning types falling under Section 4.3. is submitted, it shall be referred to the competent team/person of Sarantis for further handling and evaluation in accordance with the relevant policies and procedures.

5. How to report?

5.1. The Report, in order to facilitate its investigation and proper evaluation by the Company, shall include at least the following information:

a) personal details (name, surname, email address, phone number), if the Report is submitted eponymously;
b) date, time and location of incident(s);
c) type of misconduct;
d) the facts (data, information), including the names of people involved, names of any witnesses (if applicable), details of the incident, details of any proof, and money or assets involved.

5.2. To encourage the submission of Reports, the Company has established dedicated internal Reporting Channels that Reporting Persons may use to submit their Reports, either eponymously or anonymously. Specifically, Reports can be submitted through the following methods:

a) through the Reporting platform (hereinafter, the "**SARANTIS Group Speak Up Platform**"), which can be accessed via the Group's intranet and website (e-platform: SARANTIS Group Speak Up).
b) via email at the following address: speakup@sarantisgroup.com.

5.3. In any case, Reporting Persons are encouraged to submit their Report eponymously (i.e. under their name), in order to ensure more efficient communication with the

Whistleblowing Officer, to be able to provide any additional information or further clarifications and to facilitate the follow-up of the Report.

5.4. In the event that any third party, other than the Whistleblowing Officer, becomes a recipient of a Report, the latter is obliged to transmit it without undue delay and in any case within three (3) working days from receipt, to the designated Whistleblowing Officer, without any modification of its content or disclosure of information that may lead to the identification of the Reported Party, or a third party named in the Report.

6. Speak Up Governance

6.1. The Company has designated the Compliance and Risk Manager as the Whistleblowing Officer who is responsible for addressing and managing Reports submitted under Section 5 of this Policy. In the event of a conflict of interest involving the Whistleblowing Officer, the Whistleblowing Committee, excluding the Whistleblowing Officer, shall assume responsibility for handling the Report.

6.2. If the Report is deemed valid, the Whistleblowing Officer, in collaboration with the relevant persons or teams, shall conduct further assessment or investigation of the Report.

6.3. The Whistleblowing Committee is responsible for overseeing the Whistleblowing Process, for monitoring the investigations and determining corrective measures or actions to address the Report in coordination with the Whistleblowing Officer.

6.4. To ensure efficiency, the Speak Up Platform is operated by a third party, particularly Deloitte Business Solutions S.A., which has implemented appropriate measures to guarantee the privacy, security, and confidentiality of the Reporting Person's identity.

7. Report Handling

7.1. Upon receipt of the Report, an acknowledgment of receipt notification shall be sent to the Reporting Person within seven (7) working days. The Reporting Person shall be informed about the initial assessment (e.g., the validity) of their Report.

7.2. In any case, the Reporting Person shall be informed of the actions that have been taken within a reasonable time period, which shall not exceed three (3) months from the acknowledgement of receipt.

7.3. The Reporting Person shall be provided clear and easily accessible information on the procedures under which Reports may be submitted to external channels such as the relevant competent national authorities and, where applicable, public bodies or institutions or other bodies/agencies of the European Union.

7.4. Nothing in this Policy prohibits the Reporting Person from reporting information through external channels if they have already submitted a Report that has not been effectively addressed, or if they have reasonable grounds to believe that submitting a Report will not result in appropriate action, may lead to retaliation, or if they believe the breach could pose an imminent risk to the public interest.

8. Protection Measures for Reporting Persons

Protection of personal data

8.1. The Company takes all the necessary technical and organizational measures for the protection of personal data, adhering to high standards in its systems and the procedures under this Policy.

8.2. The processing of personal data contained in a Report is conducted in accordance with Regulation (EU) 2016/679 (GDPR) and any other relevant applicable national or European privacy and data protection legislation. The data processed include those provided in the Reports, as well as data collected during the submission, monitoring, management, archiving and reporting of Reports, actions taken to protect Reporting Persons, and the overall operation of the Reporting channel(s) and implementation of the Company's Speak Up Policy. This includes data related to Breaches of national or EU legislation and any misconduct as detailed in Section 4.2. of this Policy.

8.3. The processing of personal data in the context of the operation of the Reporting Channel(s) is carried out to ensure the Company's compliance with its legal obligations to establish Reporting Channels and implement the necessary measures for their monitoring in accordance with the Whistleblowing and Data Protection legislation.

Protection of confidential information

8.4. A basic and inviolable principle of the Policy is to protect the identity and confidentiality of the Reporting Person throughout the whistleblowing process and, if they are employees of the Group, to ensure their position and/or their professional development is not compromised. Therefore, Sarantis shall guarantee the confidentiality of the identity of the Reporting Person.

8.5. The identity of the Reporting Person shall not be disclosed without their explicit consent.

8.6. By way of derogation from Section 8.5., any information relating to a Report, including the Reporting Person's identity, may be exceptionally disclosed without their explicit consent and upon their proper, prior 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 national 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.

No Retaliation

8.7. The Company shall take appropriate measures to prohibit retaliation in any form against Reporting Persons, including threats or attempts of retaliation.

9. Diligence in keeping records

9.1. The records created and maintained in relation to Reports should be managed with a strict adherence to confidentiality principles. This means that all information, documentation, and communication related to Reports must be handled in such a way that prevents unauthorized access, sharing, or disclosure of sensitive details.

9.2. Reports shall be retained for a period that is necessary and proportionate, in accordance with relevant European Union or national legal requirements, including those concerning data protection, legal investigations, or auditing.

9.3. The Company periodically performs qualitative and quantitative analysis of data related to reports and complaints in an anonymized form, to ensure that any recurring or systemic problems and potential legal and operational risks are adequately identified and addressed.

10. False Reporting & Protection from False Reports

10.1. The Company shall protect those who submit Reports in good faith. However, it reserves the right to take action against any person involved if it is proven that at the time of submitting the Report they provided incorrect information intentionally or fraudulently.

10.2. In any event, any Reported Party who suffers damage, directly or indirectly, as a consequence of a Report submitted in bad faith, retains the protection and remedies available to them under applicable law.

10.3. Reports are deemed to have been submitted in bad faith if they are made maliciously, with culpable ignorance regarding the truth or falsehood of the allegations, and/or solely for the purpose of causing harm to the Company, Reported Parties or other persons. Employees who submit a Report in bad faith may also be subject to disciplinary sanctions or other legal measures, at the Company's discretion.

11. Policy Review & Amendments

11.1. This Policy shall be reviewed and/or amended at least on a bi-annual basis, or sooner if strictly necessary to comply with significant changes to the applicable laws or Company policy.

11.2. In this case, the most up-to-date version of the Policy is published on the Company's website: Corporate Governance (sarantisgroup.com).

12. Communication

12.1. In case you need any clarification regarding the process of submitting a Report, or any other request, you can contact the Company at the Whistleblowing Officer's e-mail address: speakup@sarantisgroup.com.

12.2. If you have any questions regarding the processing or protection of your personal data or in case you need more information about your data subject rights and how to exercise them, please contact the Company's Privacy Office via email at: DPO@sarantisgroup.com or in writing at the following postal address: 26, Amaroussiou-Chalandriou str., 151 25 Maroussi to the attention of the DPO.