



# WHISTLEBLOWING POLICY

**MARCH 2023**

<b>Author</b>	Compliance/ Finance, HR & Administration / Legal
<b>Issuing date</b>	March 2023
<b>Validation date</b>	22 March 2023

## CONTENTS

1.	INTRODUCTION.....	2
2.	DEFINITIONS.....	2
3.	PURPOSE.....	3
4.	SCOPE.....	3
5.	TYPES OF WRONGDOING.....	4
6.	REPORTING CHANNEL.....	4
7.	DIRECTIONS/GUIDELINES FOR SUBMITTING REPORTS.....	5
8.	RESPONSIBILITIES OF THE REPORTS MANAGEMENT COMMITTEE (RMC) ...	6
9.	WHISTLEBLOWERS PROTECTION.....	6
10.	RIGHTS OF WHISTLEBLOWERS AND REPORTING PARTIES .....	7
11.	INCIDENT INVESTIGATION.....	8
12.	SUPERVISION OF THE REPORTS MANAGEMENT COMMITTEE .....	8
13.	CORRECTIVE AND LEGAL ACTIONS.....	9
14.	CONFIDENTIALITY – ANONYMITY .....	9
15.	PERSONAL DATA .....	9
16.	INFORMATION AND TRAINING .....	10

## 1. INTRODUCTION

The company "Special Financial Solutions Single Member Societe Anonyme" (the "Company") adopts the present Whistleblowing policy (the "Policy") which is in line with the provisions of Law 4990/2022 (incorporating EU Directive 2019/1937). This policy contributes to the strengthening of integrity, transparency and accountability as well as to the protection of employees and the interests of the Company.

The Company encourages the submission of confidential or anonymous reports of illegal actions that may be taking place within the Company through the established reporting channels. Reports are handled and investigated with objectivity and independence. The Company assures that the whistleblowers will be protected from any retaliation and that the personal data of all parties involved is protected.

Whistleblowers should at least have reasonable suspicion and believe that what their report is valid and true. Malicious reports are prohibited. In this case the whistleblower is not protected while the reported person may exercise his/her legal rights.

## 2. DEFINITIONS

Electronic Platform: A specially designed platform accessible online via computer or mobile device at the link <http://sfs.sec.fraudline.gr>

External Parties: Third parties contractually linked to the Company, including their staff, such as consultants, contractors, subcontractors, suppliers, partners, and shareholders.

Frivolous report: The report which is obviously ungrounded and exaggerated.

Good Faith: The whistleblower has reasonable grounds to believe that the information on breaches reported was true at the time of report.

Malicious Report: A report made with the knowledge of the whistleblower that it is untrue.

Report: Internal provision of information, either verbally or in writing, regarding violations within the Company.

Repeated report: The report regarding an incident that has already been reported by the same person in the past and does not include new information.

Reports Management Committee (RMC): The committee responsible for managing reports, consisting of four regular members (Compliance Officer, Legal Counsel, Head of Internal Audit and Finance Human Resources and Administration Manager).

Responsible for Receiving and Monitoring Reports (RRMR): The Compliance Officer

Retaliation: Any direct or indirect act or omission that causes or may cause unjustified damage to the Whistleblower in an outside the workplace due to an internal report.

Whistleblower: The natural person who reports or discloses information about violations obtained in the course of their work-related activities.

### **3. PURPOSE**

The purpose of the Policy is to:

- a) define the principles and framework of whistleblowing reporting in the Company.
- b) encourage those covered by the scope of the Policy to submit a report in case an illegal or unethical behavior in the company comes to their notice.
- c) achieve the prevention and timely management of violations within the Company.

### **4. SCOPE**

Whistleblowers can be:

- A. The members of the Board of Directors and its Committees, as well as all employees (current and former), of fixed or indefinite duration or with another employment relationship or mandate, seasonal staff and interns. The same applies to those who report violations based on information obtained during the recruitment process or at another stage of pre-contract negotiation.
- B. Third parties contractually linked to the Company as well as their staff (referred to in this policy as "external partners") and specifically consultants, contractors, subcontractors, suppliers and all kinds of partners as well as the shareholders.

In order to be covered by the Policy, the report must be made in good faith. Whistleblowers must have reasonable grounds to believe, based on the circumstances and information available to them, that the information they provide is true. Good faith is presumed unless it is proven that the report was made maliciously. In the event of a malicious report, the protection described in the Policy is not provided.

## **5. TYPES OF WRONGDOING**

In case that someone of those in scope of the present policy becomes aware that one of the following wrongdoings is occurring, s/he must immediately proceed to reporting:

- Fraud,
- Corruption/Abuse of Power,
- Bribery,
- Conflict of interests,
- Theft/ Embezzlement
- Forgery,
- Money laundering,
- Violation of competition law,
- Violations in accounting, tax and control issues,
- Security breach,
- Violation of public procurement legislation,
- Violation of environmental legislation,
- Violation of consumer protection legislation,
- Breaches of confidentiality,
- Violation of personal data protection legislation,
- Discrimination, Violence and Harassment in the workplace.

The reporting policy does not cover:

- Disagreements on issues concerning policies and decisions of the management
- Personal issues and disagreements with colleagues or supervisors
- Rumors

## **6. REPORTING CHANNEL**

Any employee who suspects that any of the above wrongdoings is occurring, may optionally contact their direct supervisor. If he/she has concerns (e.g. fear retaliation or suspicion that the supervisor is involved), he/she can contact the Responsible for Receiving and Monitoring Reports (Compliance Officer) in person or in writing. Individuals may submit a report to the Electronic Platform anonymously or by name. The platform link is at the web address

<http://sfs.sec.fraudline.gr>. The platform is accessible via computers and mobile devices connected to the internet.

External Partners who wish to submit a report use the Electronic Platform anonymously or by name.

The Electronic Platform meets all technical security specifications in order to preserve the confidentiality and anonymity of all involved. Technical maintenance support through an open line of communication between the whistleblower and the members of the Reports Management Committee is provided while maintaining anonymity if desired.

Employees and external parties can submit a report to the National Transparency Authority.

## **7. DIRECTIONS/GUIDELINES FOR SUBMITTING REPORTS**

The following are general guidelines and directions for reporting:

- a. Reporting of misconduct should be done in good faith and without due delay, as soon as it is noticed.
- b. The report must be clear, specific and contain as much information and details as possible to make it easier to investigate. It should include at least the name of the person or persons who committed the misconduct, the type of misconduct, the date/time period and place where the incident took place and a detailed description of the misconduct.
- c. Sensitive personal data and information not related to the incident should not be included in the report. Sensitive data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data processed solely to identify a human being, health-related data, data concerning a person's sex life or sexual orientation.
- d. The Whistleblower need not be absolutely sure about the soundness of the report. Reasonable suspicion is enough in order to proceed to a report. He/she must not engage in illegal actions that may put himself/herself, the company or a third party at risk in order to seek and collect more evidence to support his report.
- e. The Whistleblower should be available, either confidentially or anonymously through the Electronic Platform, to provide further information if requested.

## **8. RESPONSIBILITIES OF THE REPORTS MANAGEMENT COMMITTEE (RMC)**

The reports submitted through the reporting channels are managed by the Reports Management Committee, which consists of four regular members (Compliance Officer, Legal Counsel, Head of Internal Audit and Finance Human Resources and Administration Manager) Head of the Committee and Responsible for Receiving and Monitoring Reports is the Compliance Officer. The RMC is accountable to the Board of Directors.

The RMC has the following responsibilities:

- Receives the reports.
- Examines whether they are admissible and evaluates them.
- Communicates with the Whistleblower as provided.
- Maintains a Reports Register, as referred to in Article 7 of the Whistleblowing Reports Management and Investigation Procedure.
- Plans and conducts the investigation of reports in order to prove their reliability and prepares the investigation report.
- Informs the Board of Directors on the cases investigated.

## **9. WHISTLEBLOWERS PROTECTION**

The Company protects all those included in Article 4 who report wrongdoings in good faith. In this context, any kind of retaliation against anyone who has submitted a report is prohibited, even if the report is later proven wrong.

Indicatively, the following reprisals are prohibited:

- suspension, dismissal or other equivalent measures,
- demotion, or withholding of promotion;
- transfer of duties, change of place of work, reduction of salary, change in working hours,
- withholding of training,
- negative performance evaluation or employment reference
- reprimand, imposition of disciplinary or other measure, including financial penalty,
- coercion, intimidation, harassment or marginalization;

- discrimination or unfair treatment,
- not converting a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
- non-renewal or early termination of a temporary employment contract,
- intentional harm, including reputational damage, especially on social media, or financial loss, including business loss and loss of income;
- blacklisting, which may entail that the person will not find employment in the sector or industry in the future.

In case of a malicious report, the above protection does not exist.

The same level of protection applies to individuals related to the whistleblowers, who could be subject to retaliation in an employment context, such as colleagues or relatives of the whistleblowers.

In the event that the whistleblower is an external partner, early termination or cancellation of a contract for goods or services as a result of the report is not permitted.

Any act of retaliation should be reported immediately to the RMC and it shall be investigated and resolved. If the investigation reveals that retaliation has indeed occurred, disciplinary action will be taken against the perpetrator. The person accused of retaliating has the burden of proving that his/her actions are unrelated to the employee's report (reversal of the burden of proof).

## **10. RIGHTS OF WHISTLEBLOWERS AND REPORTING PARTIES**

The Whistleblower must be informed of the receipt of his/her report, at the latest within seven (7) working days. He is also informed of the progress or result of the investigation, within three (3) months of its submission and when the investigation is completed. The Company bears the corresponding obligation to inform the whistleblower.

The reported person has the right to be informed about the wrongdoing for which he/she is accused, about some elements of the file from which the identity of the whistleblower cannot be deduced, as well as about the processing of his/her personal data. In addition, he has the right to be heard. However, if there is a serious risk that the above information could hinder



the investigation of the case and the collection of the necessary evidence or could lead to the identification of the whistleblower, the right to be informed is postponed until this risk ceases to exist.

If the report is deemed unfounded, the person referred will not be informed that there was a report against him, for reasons of protecting the working environment within the Company.

If the report is found to be malicious and the reported party has become aware of the content of the report as part of the investigation, then the latter has the right to be informed of the identity of the whistleblower (provided the report was in name), in order to exercise his rights.

## **11. INCIDENT INVESTIGATION**

During the investigation all the persons involved are treated according to the principles of equality and justice. In any case, the presumption of innocence and the right to a prior hearing apply and the confidentiality of information is protected. The investigation begins and is completed as soon as possible after the submission of the report and its subsequent evaluation.

The RMC undertake the investigation of the report and depending on the subject of the report and the seriousness of the case, a member may take over as coordinator. Where deemed necessary and depending on the subject of the investigation, additional professional support will be obtained from company executives or from external partners, such as legal advisors, auditors, fraud investigators, IT experts and specialized experts.

All those mentioned in the scope must cooperate with the RMC during the internal investigation and provide information they have.

## **12. SUPERVISION OF THE REPORTS MANAGEMENT COMMITTEE**

The RMC is supervised by the Board of Directors. The Board of Directors is informed of the outcome of the investigation and takes the final decision in relation to the recommendations of the RMC included in the investigation report.

### **13. CORRECTIVE AND LEGAL ACTIONS**

The company shows zero tolerance towards the wrongdoings referred to in article 5 hereof. Depending on the results of the investigation, the RMC recommends to the Board of Directors taking corrective or even disciplinary/legal action. Such actions may include (indicative and not limited to): (a) establishment of new internal control mechanisms, (b) modifications to existing policies and/or procedures, (c) additional employee training, (d) imposition of disciplinary sanctions, (e) legal actions, including litigation of any civil claims and seeking criminal liability.

### **14. CONFIDENTIALITY – ANONYMITY**

The Company encourages employees and external partners to raise concerns about potential wrongdoing through existing reporting channels. Named confidential reports are encouraged. However, it is clarified that anonymous reports are treated with the same attention and seriousness.

The company also undertakes to make every effort, and to take every appropriate measure, to protect the identity of both the Whistleblower and the reported party as well as third parties involved and to handle the case with complete confidentiality and secrecy. The internal investigation is conducted under conditions of discretion and the confidentiality of the information is protected in every appropriate way, even if the specific circumstances require a thorough investigation.

In any case, during the management and investigation of an incident, the identity of the Whistleblower (provided the report is by name) is not disclosed to anyone other than the authorized persons responsible for receiving, monitoring and investigating the reports, unless the Whistleblower has given express consent or the report proves to be malicious.

Anonymity is achieved through the use of appropriate technical and organizational measures and mainly through the Electronic Platform, which supports anonymous and two-way communication and meets high security standards.

### **15. PERSONAL DATA**

Any processing of personal data under this Policy is carried out in accordance with the national and European legislation applicable to personal data (Regulation 2016/679 of the European Union [General Data Protection Regulation] and Greek Law 4624/2019) and the Company's

personal data protection policy. The data of all involved are protected and are subject to processing exclusively in relation to the occasional report and for the only purpose of identifying the soundness or not of the report and investigating the specific incident.

The Company takes all necessary technical and organizational measures to protect personal data. Access to the data included in the reports can have only those involved in the management and investigation of the incident, such as members of the RMC, the Board of Directors (to the extent absolutely necessary for the decision-making process), specialized external consultants in the context of the investigation. Sensitive personal data and other data not directly related to the report are not further processed.

The manner of exercising and the conditions for limiting the rights of data subjects in reports are described in article 8 of the Whistleblowing Reports Management and Investigation Procedure.

Personal data is deleted within a reasonable period of time from the completion of the investigation. Personal data is deleted from the Report Register, from the material resulting from the investigation and from the reporting platform, in accordance with the time frames set out in Article 8 of the Whistleblowing Report Management and Investigation Procedure.

## **16. INFORMATION AND TRAINING**

All employees and external partners must comply with this Policy. The RMC ensures that the Company's employees are informed and trained on the content of this policy. Information is provided either in person, or through electronic training, sending informative material, email or in another appropriate way depending on the category of employees and external partners. Also, information about the policy is published on the Company's Procedures common folder as well as on the reporting platform.