

## WHISTLEBLOWING POLICY

## Contents

1. Purpose
2. Scope of the Law and Policy
3. Subjective Scope of the Law and Policy
4. Guiding Principles
5. Submission and Receipt of Reports
6. Investigation of Reports
7. Personal Data
8. Security and data storage/archive

## 1. Purpose

- 1.1. The purpose of this document is to ensure that the company named "TRADE SUPPORT AND DISTRIBUTION, STORAGE AND DISTRIBUTION SERVICES COMPANY S.A." with the distinctive title 'M.S.P.S. S.A.'. (hereinafter "the Company") has an appropriate procedure for receiving, recording and processing confidential, named or anonymous complaints from those entitled to make them, for the purpose of reporting incidents in accordance with Law 4990/2022 which transposed Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting violations of Union law (L 305).
- 1.2. The Company's main priority is to maintain high standards of transparent operation, always with respect to its employees, directors, managers, executives, as well as any other involved-stakeholders in society.
- 1.3. The Company recognizes that all employees need accessible and reliable channels to report wrongdoing, strong protection against retaliation of any kind, as well as mechanisms to receive complaints and reports.

## 2. Scope of the Law and Policy

The provisions of the Policy apply to the protection of persons who report or disclose:

- 2.1. Infringements of Union law, as more specifically defined in Part I of the Annex to the Directive, in the areas of:
  - ✓ of public procurement,
  - ✓ financial services, products and markets, as well as the prevention of money laundering and the financing of terrorism,
  - ✓ product safety and compliance,
  - ✓ transport security,
  - ✓ environmental protection,

- ✓ radiation protection and nuclear safety,
  - ✓ food and feed safety, and animal health and welfare,
  - ✓ public health,
  - ✓ consumer protection,
  - ✓ the protection of privacy and personal data, and the security of network and information systems,
- 2.2. Infringements affecting the economic interests of the Union referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU) and in particular those set out in the relevant union measures,
- 2.3. Violations related to the internal market, as referred to in par.2 of Article 26 of the Treaty on the Functioning of the European Union (TFEU), including violations of Union rules on competition and State aid, as well as violations relating to the internal market concerning acts that infringe the rules on corporate taxation or arrangements whose purpose is to secure a tax advantage that frustrates the object or purpose of the applicable legislation on corporate taxation.

### 3. Subjective Scope of the Law and Policy

- 3.1 The provisions of the Policy apply to: those who are employed and have acquired, in the course of their work, information about violations that they report, and in particular:
- ✓ to the Company's employees regardless of whether their employment is full or part-time, permanent or seasonal, or whether they are seconded from another institution.
  - ✓ to non-employed persons, self-employed persons or consultants or home workers,
  - ✓ to shareholders and persons belonging to the administrative, management or supervisory body of a company, including non-executive members, as well as volunteers and paid or unpaid interns,
  - ✓ to any persons working under the supervision and instructions of contractors, subcontractors and suppliers,
  - ✓ to persons who publicly report or disclose information about violations obtained in the context of an employment relationship that has ended for any reason, including retirement, and to reporters whose employment relationship has not yet begun, in cases where information about violations has been obtained during the recruitment process or at another stage of pre-contract negotiations.
- 3.2. The measures for the protection of interests provided for in this Policy also apply, where appropriate, to:

- ✓ intermediaries,
- ✓ third parties associated with the petitioners who may be subject to retaliation in a work context, such as colleagues or relatives of the petitioners; and
- ✓ partnerships or legal entities in which the petitioners have an interest, or for which they work, or with which they are otherwise connected by an employment relationship.

## 4. Guiding Principles

The basic principles underlying this are the following:

- 4.1. Reporting infringements must be protected by the Company whether they are anonymous or named complaints.

Persons who provide additional information in relation to a complaint, as well as those who assist or seek to assist in the investigation may be considered as petitioners entitled to protection.

In this context, any kind of negative behavior against anyone who has made a report is prohibited, even if the report is subsequently proven to be incorrect.

The same level of protection applies to third parties connected to the petitioners who could be retaliated against in a work context, such as colleagues or relatives of the petitioners.

If the reporting party is an external partner, early termination or cancellation of a contract for goods or services as a result of the report is not allowed.

Violation reporters are entitled to protection if, at the time of reporting, they had reasonable grounds to believe that the information about the reported violations was true and within the scope of this Policy.

Protection should be afforded for disclosures made in the reasonable belief that the information is true at the time of disclosure.

The protection extends to those who disclose inaccurate information with excusable error and continues to apply after the accuracy of the disclosure has been assessed.

Knowingly untrue disclosures are not protected.

- 4.2. A person who makes a disclosure and it is proven to have been knowingly untrue is subject to sanctions and civil liability.
- 4.3. Persons who have reported or made public information about violations anonymously but were subsequently identified and retaliated against are entitled to the protection provided by the provisions of Directive 2019/1937 (EU) if the conditions of article 6(3) (article 7(3) of Law 4990/2022) are met.
- 4.4. According to Law 4990/2022, personal data and any kind of information leading, directly or indirectly, to the identification of the petitioner, shall not be disclosed to anyone other than the authorized staff members who are responsible for receiving or monitoring the reports, unless the petitioner consents thereto.

By way of derogation from par. 1, the identity of the petitioner and any other

information may be disclosed only in cases required by EU or national law, in the context of investigations by competent authorities or in the context of judicial proceedings, and if this is necessary to serve the purposes of Law 4990/2022 or to safeguard the rights of defense of the petitioner.

The Company undertakes to maintain the anonymity of the petitioner, as well as other parties involved and to refrain from actions that may result in the disclosure of their identity. However, it is noted that disclosure of the identity of the petitioner and any other information may be required by judicial or legal or other investigative proceedings as part of the investigation of the case.

Disclosures shall be made after informing the reporting party in writing of the reasons for the disclosure of its identity and other confidential information, unless such information would undermine investigations or judicial proceedings.

After being informed, the reporting party shall have the right to submit written comments to the authority or body making the disclosure, which shall not be disclosed to any person. Except where the grounds for the comments are considered insufficient, the identity and other confidential information of the reporting party shall not be withheld. This shall be without prejudice to further safeguards of the identity of the petitioner and the information from which it may be derived, provided for by specific provisions of Union or national law.

- 4.5. Reports will be examined with due diligence, impartial judgment and objectivity and in case the complaints are confirmed, the Company shall take all appropriate corrective measures. Anonymous reports shall be considered according to the quality of their documentation and the possibility provided to identify the irregular action complained of.
- 4.6. Reports are made without the promise of payment or the existence of any consideration. In the event that the reporting party was involved in the event, he/she will not be relieved of his/her responsibilities, but his/her contribution to the detection and investigation of irregularities, omissions or criminal acts will be taken into account.
- 4.7. The Company respects the fundamental rights of the individuals involved in a report and ensures that the actions and procedures provided for are in accordance with the applicable legislation.
- 4.8. The rights and remedies provided for in Directive 2019/1937 (EU) are not waived or limited by any individual agreement, policy, form or term of employment.
- 4.9. Reporting parties who have made a report in good faith in accordance with paragraph 4.3 shall be protected from any acts of retaliation, discrimination or other forms of unfair treatment, regardless of the outcome of the investigation of the report.

According to Article 17 of Law 4990/2022, any form of retaliation against the persons referred to in Article 6 of the law is prohibited, including threats and acts of retaliation.

In particular, the following forms of retaliation shall be prohibited:

- ✓ suspension, dismissal or equivalent measures,
- ✓ demotion, failure to promote or deprivation of promotion,

- ✓ removal of duties, change of place of work, reduction of salary, change of working hours,
- ✓ training deprivation,
- ✓ negative performance appraisal or negative job recommendation,
- ✓ reprimand, disciplinary or other measure, including a financial penalty,
- ✓ coercion, intimidation, harassment or marginalization,
- ✓ discrimination, disadvantage or unfair treatment,
- ✓ failure to convert a temporary employment contract into a permanent contract,
- ✓ non-renewal or early termination of a temporary employment contract,
- ✓ intentional harm, including damage to reputation, in particular on social media, or economic loss, including business loss and loss of income,
- ✓ blacklisting, based on a sectoral or industry formal or informal agreement, which may imply that the person will not find a job in the sector or industry in the future,
- ✓ early termination or cancellation of a contract for goods or services,
- ✓ revocation or cancellation of a license or permit,
- ✓ referral for psychiatric or medical treatment,
- ✓ refusal or denial of reasonable accommodation to persons with disabilities.

## 5. Submission and Receipt of Reports

- 5.1. The Company has an updated and detailed procedure for the management of reports and complaints in accordance with the latest standards.
- 5.2. The Company has designated Human Resources (HR) Director of the company as the company's dedicated reporting channel to whom both named and anonymous reports can be submitted.

Contact details:

- Name: Anastasia Floka
- Phone: 2109604200
- E-mail: [whistleblowing@msps.net](mailto:whistleblowing@msps.net)

HR Director (a) receives the petitions and maintains communication with the petitioner, (b) monitors the progress of the petitions, and (c) informs the petitioner of developments.

In particular, HR Director has the following responsibilities:

- ✓ provides appropriate information about the possibility of reporting within the Company and communicates this information in a prominent place within the Company,

- ✓ receives reports of violations falling within the scope of the Policy,
- ✓ acknowledge receipt of the report to the petitioner within seven (7) working days from the date of receipt,
- ✓ take the necessary steps for the competent bodies of the Company to deal with the report, or close the procedure by filing the report, if it is incomprehensible or improperly submitted or does not contain facts that constitute a violation of EU law or there are no serious indications of such a violation and the notification of the relevant decision to the petitioner, who, if he considers that it has not been dealt with effectively, may resubmit it to the EAD, which, as an external channel, exercises the powers of Article 12 of Law 4990/2012,
- ✓ ensure that the confidentiality of the identity of the reporter and any third party named in the report is protected by preventing access to it by unauthorized persons. HR Director treats all written reports as confidential and is bound by an obligation to maintain the confidentiality of the information contained in each report.
- ✓ monitors the reports and maintains contact with the petitioner and, if necessary, requests further information from the petitioner,
- ✓ shall inform the petitioner of the action taken within a reasonable period of time, which shall not exceed three (3) months from the acknowledgement of receipt, or if no acknowledgement has been sent to the petitioner, three (3) months from the expiry of seven (7) working days from the submission of the report,
- ✓ provides clear and easily accessible information on the procedures under which reports can be submitted to the EDPS and, where appropriate, to public bodies or institutions or other bodies or agencies of the European Union; and
- ✓ designs and coordinates training activities related to ethics and integrity, participates in the development of internal policies to enhance the integrity and transparency of the Company.

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

- ✓ Misconduct should be reported in good faith and without delay, as soon as it comes to the attention of the party concerned.
- ✓ The report should be clear, defined and contain as much information and detail as possible to facilitate its investigation. It is therefore impossible to investigate a report any further if it is not specific or if it contains only very general allegations without further clarification.
- ✓ The report should include at least the name of the person (or persons) who may have committed misconduct, the date/time period and place where the incident took place, the group company to which the incident relates, whether



other persons are aware of suspicions about the matter, whether management is aware of the matter, whether the reporting party is aware of any attempt to conceal the misconduct, the nature of the misconduct and as detailed a description of it as possible and whether there are documents supporting the report.

- ✓ Personal data, including sensitive data, and more generally information that is not related to the incident should not be included in the report. If not included, it shall be deleted.
- ✓ The petitioner does not need to be absolutely certain of the validity of his/her report. It is sufficient to maintain reasonable concerns or suspicions. He/she should not take illegal actions that may put himself/herself, the company/group or a third party at risk in order to seek and gather more evidence to support his/her report.
- ✓ The submission of anonymous confidential reports is encouraged so that further information can be contacted and provided if requested and necessary. Anonymous reports may make it difficult or impossible to investigate and assess the credibility of the report. However, it is clarified that anonymous reports are treated with exactly the same care and weight as anonymous reports.
- ✓ Blatantly unfounded reports will not be investigated further.

5.4. The Company's employees have an obligation to report any action or violation that comes to their attention. Failure by a staff member to report illegal activity, violation of regulations or even a suspected violation of the above is misconduct and will be treated as such.

5.5. If an employee of the Company or a third party has doubts about the need to report an irregularity, omission or criminal act or suspicion thereof, or wishes clarification regarding his/her protection or other matters, and his/her questions are not covered herein, he/she may direct his/her questions to HR.

## 6. Investigating Reports

- 6.1. The investigation of the validity of the facts described in the report is the responsibility of the Audit Committee which consists of: Chief Executive Officer, General Manager, Chief Commercial Officer.
- 6.2. The Audit Committee is charged with conducting a timely and thorough investigation, in accordance with the principles of impartiality, fairness and respect for the confidentiality of all persons involved.
- 6.3. In the framework of the investigation, the Audit Committee may address the relevant competent departments of the company and, if it deems necessary, external consultants with expertise in the subject of the submitted report, provided that their participation serves the investigation of the report, while ensuring confidentiality.

- 6.4. Transparency in the investigation of the complaint is a basic principle and the Company is committed to providing the appropriate means (technical and organizational, among others) for the successful and transparent management of the reports, without delay.
- 6.5. After the completion of the investigation process, the Audit Committee prepares a report on the investigations carried out and the evidence obtained and determines the actions to be taken.
- 6.6. Otherwise, if the completion of the investigation reveals the absence of sufficiently substantiated evidence or, at least, the unsubstantiated nature of the evidence relied on in the report, the report shall be filed together with the relevant justification.
- 6.7. Everyone involved in the receipt and investigation has the right of full access to the file where the report/complaint is kept, if applicable. Each party involved undertakes to strictly maintain the confidentiality of all information of which they are aware in the context of the investigation in question.
- 6.8. In investigating the report, the Commission is committed to:
  - ✓ ensure the confidentiality of the identity of the petitioner and not expose the petitioner to retaliation,
  - ✓ ensure that the risk of the reported incident continuing is minimized,
  - ✓ prevent any further property damage to the Company or any reputational impact of the incident,
  - ✓ prevent any further property damage to the Company or any reputational impact of the incident,
  - ✓ to ensure the confidentiality and integrity of evidence and its sources, and to treat with discretion any information received

## 7. Personal data

Any processing of personal data under this policy, including the exchange or transmission by the competent authorities, is carried out in accordance with national and European data protection legislation, including any specific legislative provisions and the harmonized data protection policy of the Company, which takes all necessary technical and organizational measures to protect personal data.

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

Only those involved in the management and investigation of the incident can have access to

the data contained in the reports.

The personal data contained in the Reports may be disclosed to the corporate bodies and the internal departments that are competent in each case, as well as to the judicial authorities, in order to initiate the necessary procedures for taking, on the basis of the Report, adequate judicial and/or disciplinary protection measures against the reported person(s), in case the information collected and the investigation reveals the validity of the reported facts. In such cases, the data may also be disclosed to qualified external persons.

When carrying out activities to check the validity of the report, all necessary measures shall be taken to protect the data against accidental or unlawful destruction, loss or unauthorized disclosure (notification).

The Company, as the Data Controller, by derogation of paragraph a' of par. 1 of Article 5, Articles 12 and 13, paragraphs (a) to (b) of Article 5, Articles 12 and 13, paragraphs (c) to (d) of Article 5, Article 12 and 13. 1 to 4 of Article 14 and Article 34 of the General Data Protection Regulation does not provide relevant information on the processing of personal data to the reporting party and any third person in his capacity as data subject named in the report or the personal data resulting from monitoring measures and in particular on the source of origin in accordance with paragraph f' of Paragraph 5 of the General Data Protection Regulation. 2 of Article 14, pursuant to paragraph 2 of Article 14. 5 of the same Article in conjunction with Article 23 of the General Data Protection Regulation (GDTR), for as long as necessary and to the extent necessary for the purpose of preventing and responding to attempts to obstruct the report, obstruct, frustrate or delay the monitoring measures, in particular with regard to investigations or attempts to identify the petitioners, and to protect them against retaliation.

The Company may not satisfy the rights granted by Articles 15 to 22 of the GDTR, when they are exercised by the named persons and third parties named in the report, or have resulted from monitoring measures as defined in par. 5 5.

## 8. Security and data storage/archive

- 8.1. The Company will record all reports received under the policy and will retain them for as long as it considers the processing necessary and proportionate to the purpose pursued and in any case until the completion of any investigation or judicial or other legal proceedings initiated as a consequence of the report against the reporting party, the Interested Party or third parties. Furthermore, the documents relating to the report shall be kept, both in paper and electronic form, for a period not exceeding the time necessary for the proper completion of the procedures provided for in this Policy and in any case until the conclusion of any judicial or other legal proceedings in relation thereto.
- 8.2. If - on the basis of the collected data - a disciplinary sanction is imposed on the reported person or if there are other reasons that justify and require the extension of the storage of the data concerning the reported person, these data will be stored and, if it is a company employee, will be kept in the employee's file in the personnel department's archive.