Whistleblowing Policy

Purpose

Musala Soft is committed to complying with the applicable foreign and domestic laws, satisfying the Company's Code of Conduct, and particularly to ensuring that business is conducted with integrity and that the Company's financial information is accurate.

If potential violations of Company policies or applicable laws are not recognized and addressed promptly, the Company and those working for or with the Company could face governmental investigation, prosecution, fines, and other penalties. Consequentially, and to promote the highest ethical standards, the Company will maintain a workplace that facilitates the reporting of potential violations of Company policies and applicable laws.

All employees or any other person including vendors, contractors, subcontractors, consultants, trainees, shareholders, former employees, job applicants and any other third parties (collectively referred hereinafter as "Person(s)") must be able to raise concerns regarding such potential violations easily and free of any fear of retaliation.

Definition of whistleblowing

Whistleblowing is the internal or external reporting or public disclosure of breaches of Bulgarian and European Union law. The material scope of this Policy is outlined in Schedule 1 hereto.

Where persons report information on breaches or make a public disclosure in accordance with this policy and the relevant legislation they shall not be considered to have breached any restriction on disclosure of information and shall not incur liability of any kind in respect of such a report or public disclosure provided that they had reasonable grounds to believe that the reporting or public disclosure of such information was necessary for revealing a breach pursuant to this Directive.

Reporting persons shall not incur liability in respect of the acquisition of or access to the information which is reported or publicly disclosed, provided that such acquisition or access did not constitute a self-standing criminal offence. In the event of the acquisition or access constituting a self-standing criminal offence, criminal liability shall continue to be governed by applicable national law.

Any other possible liability of reporting persons arising from acts or omissions which are unrelated to the reporting or public disclosure or which are not necessary for revealing a breach pursuant to this Directive shall continue to be governed by applicable Union or national law.

Personal scope

1. This Policy applies to the following reporting persons working in Musala Soft and its subsidiaries who acquired information on breaches in a work-related context:
   a) any employees of Musala Soft and its subsidiaries;
   b) persons having self-employed status, who are in a work relationship with Musala Soft and its subsidiaries;

c) volunteers and paid or unpaid trainees;
d) shareholders and persons belonging to the management or supervisory body of an undertaking, including non-executive members;
e) any persons working under the supervision and direction of contractors, subcontractors and suppliers.

2. This Policy shall also apply to reporting persons where they report or publicly disclose information on breaches acquired in a work-based relationship which has since ended.
3. This Policy shall also apply to reporting persons whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.
4. The measures for the protection of reporting persons set out below shall also apply, where relevant, to:

a) facilitators;
b) third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons; and
c) legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context.

Conditions for protection of reporting persons

1. Reporting persons shall qualify for protection under this Policy provided that:

a) they had reasonable grounds to believe that the information on breaches reported was true at the time of reporting; and
b) they reported either in accordance with this Policy and the relevant legislation.

2. Proceedings shall not be instituted for reports relating to violations committed more than two years ago.

Duty to report

Everyone is required to report to the Company any suspected violation of any law that applies to the Company and any suspected violation of the Company's Code of Conduct when there are reasonable grounds for it. This includes possible accounting or financial reporting violations, insider trading, leak of unpublished sensitive information, bribery, or violations of the anti-retaliation aspects of this Policy. Retaliation includes adverse actions, harassment, or discrimination relating to the report of a suspected violation.

Reporting is crucial for early detection, proper investigation and remediation, and deterrence of violations of Company policies or applicable laws. There should not be fear of any negative consequences for reporting reasonably suspected violations because retaliation for reporting suspected violations is strictly prohibited by Company policy. Failure to report any reasonable belief that a violation has occurred or is occurring is in itself a violation of this Policy and such failure will be addressed with appropriate disciplinary action, including possible termination of employment.

How to Report

Concerns may be reported in written form, including via email, or orally via the phone, or in a live meeting, to the operational line manager or People Care at people.care@musala.com.

The reports should be documented in accordance with the prerequisites pointed out in the national legislation of Bulgaria and must include at least the following:

1. the sender's name, address, and phone number, as well as an email address, if any;
2. the names of the person against whom the report is filed and his workplace, if the report is filed against specific persons and they are known;
3. specific details of a violation or of a real danger that it will be committed, place and period of the violation, if it was committed, a description of the act or the situation, and other circumstances, as far as these are known to the reporting person;
4. date of submission of the signal;
5. signature, electronic signature, or other identification of the sender.

The submitter may be contacted for further information. Any supplementary documents that are relevant to the report and support the claims can be submitted together with the signal.

Further steps

The reporting person will be notified of the receipt of the report within seven days of that receipt. If the signal does not meet the specified requirements, the reporting person will be asked to eliminate the irregularities within seven days. If the irregularities are not corrected within this period, the signal is returned to the reporting person along with its attachments.

All reports under this Policy will be promptly and appropriately investigated within a reasonable timeframe not exceeding three months following the confirmation of receipt, and all information disclosed during the course of the investigation will remain confidential, except as necessary to conduct the investigation and take any remedial action, in accordance with applicable law.

The authorized persons will prepare an individual report in which they briefly describe the information from the report, the actions taken, the final results of the check on the report, which, together with the reasons, will be communicated to the person who submitted the report and to the affected persons, in compliance with the obligation to protect their personal data.

Any processing of personal data carried out pursuant to this Policy, including the exchange or transmission of personal data by the competent authorities, shall be carried out in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680. Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.

Everyone working for or with the Company has a duty to cooperate in the investigation of reports of violations. Failure to cooperate in an investigation, or deliberately providing false information during an investigation, could be a base for disciplinary action, including termination of employment. If, at the conclusion of its investigation, the Company determines that a violation has occurred, the Company will take effective remedial action commensurate with the nature of the offense. This action may include disciplinary action against the accused party, up to and including termination. Reasonable and necessary steps will also be taken to prevent any further violations of Company policy.

Musala Soft creates and maintains a register of reports of violations, which is not public.

External reporting

In view of the possibility of quickly preventing a violation or removing the consequences of such a violation, the signal should be submitted as a priority through an internal reporting channel.

If there is a reasonable assumption that there is a risk of retaliatory, discriminatory actions for the reporting person, and that no effective measures will be taken to verify the report, the report may be submitted through an external submission channel.

The disclosing party can make an oral or written communication of information on breaches to the designated competent national authorities. The Bulgarian central external reporting authority is the Commission for Personal Data Protection.

Public disclosure

1. A person can make a public disclosure making the information on breaches available in the public domain if any of the following conditions is fulfilled:

a) the person first reported internally and externally, or directly externally in accordance with Chapters II and III, but no appropriate action was taken in response to the report within the timeframe referred to in point (f) of Article 9(1) or point (d) of Article 11(2); or
b) the person has reasonable grounds to believe that:
    i. the breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage; or
    ii. in the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach.

Non-retaliation

There shall not be any adverse action against any Person for complaining about, reporting, or participating or assisting in the investigation of a reasonably suspected violation of any law, this Policy, or the Company's Code of Conduct. The Company takes reports of such retaliation seriously. Incidents of retaliation against any Person reporting a violation or participating in the investigation of a reasonably suspected violation will result in appropriate disciplinary action against anyone responsible, including possible termination of employment. Those working for or with the Company who engage in retaliation against reporting Persons may also be subject to civil, criminal and administrative penalties.

Record keeping and document retention

Musala Soft will keep records of every report received. Oral reports shall also be recorded and the reporting person shall be offered the opportunity to check, rectify and agree with the recording or the minutes of the conversation by signing them. All documents related to reporting, investigation and enforcement pursuant to this Policy shall be kept in accordance with the Company's record retention policy and applicable law.

Further information

The information about the terms and conditions for submitting reports is provided on the website of Musala Soft, as well as in its offices and workplaces.

You can find further information on the topic of whistleblowing in Directive (EU) 2019/1937 and the relevant local legislation.

Schedule 1

This Policy lays down common minimum standards for the protection of persons reporting the following breaches of Bulgarian and European Union law:

a) breaches of Bulgarian legislation in the field of the rules for payment of public state and municipal receivables;
b) breaches of employment legislation;
c) breaches of the legislation related to the performance of public service;
d) breaches falling within the scope of the Union acts that concern the following areas:
    (i) public procurement;
    (ii) financial services, products and markets, and prevention of money laundering and terrorist financing;
    (iii) product safety and compliance;
    (iv) transport safety;
    (v) protection of the environment;
    (vi) radiation protection and nuclear safety;
    (vii) food and feed safety, animal health and welfare;
    (viii) public health;
    (ix) consumer protection;
    (x) protection of privacy and personal data, and security of network and information systems;
e) breaches affecting the financial interests of the Union as referred to in Article 325 TFEU and as further specified in relevant Union measures;
f) breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law;
g) a committed crime of a general nature, for which a person has learned in connection with the performance of his work or through the performance of his official duties.