Regulation for Reporting Legal Violations & Taking Subsequent Actions

of the Software Mind USA & LATAM

Document Information

Document owner	Jan Antczak
Document status	Final version - published
Point of Contact	Jan Antczak

Change History

Date	Changes
11.2023	Document creation
01.2025	Content adjusted to comply with local regulations
02.2025	Minor changes, added tables with document details
02.2026	Group structure updated

1. Introduction

Software Mind Companies has set Regulation for Reporting Legal Violations & Taking Subsequent Actions hereinafter referred to as Whistleblowing Policy to be a tool for receiving complaints from both employees and third party on suspected violations of law and rules and to protect and provide fair treatment to whistleblower. Policy applies to employees and associates of Software Mind Companies in the United States and LATAM.

2. Definitions

The terms used in the provisions of the Regulation:

Company – respectively each z Software Mind Company in the United States and LATAM, in particular:

- Virtual Mind SRL (Argentina),
- Software Mind Inc. (USA),
- The Big Three 912 Inc. (USA),
- Virtual M Inc. (USA),
- Virtual Software LLC (USA),
- ProSoft LLC (USA),
- Pyxis Group Sociedad Anonima (Costa Rika),
- Number 8 Holdings LLC (USA),
- Number 8 S. De R.L. (Honduras)

Compliance Officer – the person responsible for receiving Reports and authorized to take Follow-up actions

Group Software Mind, Group – Capital Group, which includes the following Companies:

Software Mind S.A. (Poland) – parent company,

1. Software Mind Nordics Sp. z o.o. (Poland) – subsidiary,
2. ValueLogic Sp. z o.o. in liquidation (Poland) – subsidiary,
3. Chmurowisko Sp. z o.o. in liquidation (Poland) – subsidiary,
4. Software Mind Outsourcing Services Sp. z o.o. (Poland) – subsidiary,
5. SM-ALL Shared Services Center sp. z o.o. – subsidiary,
    a. Virtual Software LLC (USA),
    b. ProSoft LLC (USA)
        i. Pyxis Group Sociedad Anonima (Costa Rica),
        ii. Number 8 S. De R.L. (Honduras),
6. Software Mind, GmbH (Germany) - subsidiary,
7. Software Mind LTD (UK) – subsidiary,
8. Software Mind Inc. (USA) – subsidiary,
9. Software Mind SRL (Moldova) – subsidiary,
10. Software Mind CF SRL (Romania) – subsidiary,

11. Software Mind, S.L. (Spain) – subsidiary,
12. Core3 Sp. z o.o. (Poland) – subsidiary

Follow-up action - an action taken by Company to assess the veracity of the allegations contained in the Report and to counteract the Breach of law that is the subject of the Report, in particular by investigation, initiation of an audit or administrative proceeding, filing of a charge, action taken to recover funds or closure of the proceedings implemented under this Policy;

Retaliatory action - a direct or indirect act or omission in a Work-related context that is caused by a Report and that violates or is likely to violate the rights of the Whistleblower or causes or is likely to cause unreasonable harm to the Whistleblower, including the groundless initiation of proceedings against the Whistleblower;

Information on breaches - information, including reasonable suspicion, regarding an actual or potential Breaches of law that has occurred or is likely to occur at Company or information regarding an attempt to conceal such Breach of law;

Feedback - information provided to the Whistleblower on the Follow-up actions planned or taken and the reasons for them;

Work-related context - past, present or future work-related activities under an employment relationship or other legal relationship underlying the provision of work or services, or the performance of functions in or for Company, in the course of which Information on breaches has been obtained and the possibility of experiencing Retaliatory actions exists;

Breach of law - an act or omission that is unlawful or intended to circumvent the law concerning;

Information on breaches - information, including reasonable suspicion, regarding an actual or potential Breaches of law that has occurred or is likely to occur in Company or information regarding an attempt to conceal such Breach of law;

Employee - a person performing paid work for Company or providing work for remuneration on a basis other than employment, regardless of the basis of employment;

Whistleblower - an individual who reports Information about a Breach of law obtained in a Work-related context,

Report - Internal Report,

Policy - this Whistleblowing Policy.

3. Whistleblowing

The Regulation shall apply to an individual who reports or discloses Information on breaches obtained in a Work-related context, including:

a. an employee,
b. a person providing work on a basis other than employment, including under a civil law contract,
c. an entrepreneur,
d. a member of a body of the Company,
e. persons working under the supervision and direction of contractors, subcontractors and suppliers

All the authorized persons indicated above are encouraged and entitled to report Information on breaches such as:

a. danger to life or health,
b. danger to climate or environment,
c. corruption or other financial crime,
d. abuse of authority,
e. breach of personal data protection regulations,
f. improper performance of employee duties under applicable laws and internal regulations in force in the relevant Company,
g. unethical behavior and actions, in particular violations of the Software Mind Group's Code of Business Ethics,
h. taking actions that lead or may lead to a threat to the life and health of employees and persons cooperating with the relevant Company on another legal basis, violating the principles of occupational health and safety,
i. lack of care for the welfare of the Company or the Group and the property entrusted to it, acting to the detriment of the Company or the Group,
j. behavior that violates applicable laws,

and others, if authorized by law.

4. How and to whom do you whistle-blow

- Reports can be made through the Platform, available at the web address indicated on the website of the relevant Company.
- The entity authorized to receive Reports is the Compliance Officer.

- If the Report concerns the Compliance Officer, the Report may be sent to the e-mail address of the member of the Board of Directors of the Company to which the Report relates.
- The Report may be made confidentially or fully anonymously after selecting the appropriate option in the form.
- The Whistleblower may provide in the Report his or her personal information, in the form of: first name, last name, mailing address (i.e. street, house number, postal code, city, country), as well as indicate whether the Whistleblower is an employee of the Company where the Breach of law that is the subject of the Report occurred.
- The Whistleblower may provide his e-mail address to which he will receive notifications about the current status of the processing of the Report.
- The Report may additionally be accompanied by files documenting the Breach of law in question and a recorded voice message regarding the Breach of law in question.
- Once the Report is submitted, the Platform will automatically generate individual login credentials (username and password) for the Whistleblower, through which the Whistleblower will be able to access the login area, through which it is possible, among other things, to check the status of the processing of the Report, contact the Compliance Officer and provide further information regarding the Breach of law.
- If the reported Breach of law involves a Compliance Officer or Information Security Officer, then action in accordance with these Policy shall be taken by a designated member of the Company's governing body, excluding the Compliance Officer or Information Security Officer, respectively.

5. Investigation and Resolution

The entity authorized to take Follow-up actions is the Compliance Officer, unless the case involves a Compliance Officer, in which case the internal entity authorized to take Follow-up actions is a designated member of the governing body of the Company affected by the Report.

As part of the Follow-up action, the Compliance Officer may take actions to verify information about the Breach of law, such as, but not limited to:

a. conducting further communication with the Whistleblower, including requesting additional information,
b. receiving explanations to determine the facts of the Breach of law,
c. requesting copies of or access to documents relating to the Breach of law.

As a result of the Follow-up actions carried out, the Report may be found to be:

a. legitimate and then corrective actions are taken and/or consequences are drawn,

b. unfounded (unsupported) and then the Report is dismissed.

The Company may apply to the person who committed the Breach of law the consequences provided by law, in particular:

a. apply disciplinary consequences, including the penalty of a warning or reprimand,
b. change the terms and conditions of employment, including assigning another job,
c. terminate the employment relationship,
d. terminate a civil law contract,

6. No Retaliation

The Company shall not retaliate or attempt or threaten to retaliate against a Whistleblower or treat a Whistleblower unfavorably for making a Report.

7. Psychological support

The Company offers employees the opportunity to use free, anonymous psychological consultations, particularly in the case of an internal report. Participation in the consultation is voluntary and does not affect job performance evaluations or any other HR decisions.

8. Confidentiality

The Whistleblower's personal data and other information allowing to establish his/her identity shall not be disclosed to unauthorized persons, except with the express consent of the Whistleblower.

The above rule does not apply if the obligation to disclose the Whistleblower's personal data to the competent public authorities or courts results from the provisions of applicable law.

9. Protection of personal data

The administrator of the personal data collected and processed in connection with the receiving of the Report and taking Follow-up actions is the Company where the Report was made.

In all matters relating to the processing of personal data in connection with the processing of the Report, in particular with regard to the exercise of rights related to their processing, the Whistleblower may contact the Company via e-mail address: personal.data@softwaremind.com or in writing to the administrator's mailing address.

The Company shall make available on its website and on the platform designed for Reports information on the rules for processing personal data in connection with

receiving Reports and taking follow-up actions, as required by the relevant data protection regulations.