Regulation for Reporting Legal Violations & Taking Subsequent Actions

of the Software Mind Europe

Document Information

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

Change History

Date	Changes
11.2023	Document creation
08.2024	Content adjusted to legal requirements
01.2025	Content adjusted to comply with local regulations
02.2025	Minor changes, added tables with document details
05.2025	Changes concerning the reporting of threats to employees' health and life
02.2025	Group structure updated

Chapter I

General Provisions

§ 1

The regulations for reporting legal violations and taking Subsequent Actions within the Software Mind Capital Group (hereinafter referred to as the 'Regulation') defines:

1. the scope of the field of Violation Reports subject to consideration in accordance with the principles outlined in the Regulations;
2. the methods of submitting Reports using the internal channel;
3. individuals authorised to report Violations;
4. the organisation of receiving and verifying Reports;
5. actions taken by the Company to verify information about Violations;
6. principles of protecting Authorised persons;
7. taking Subsequent Actions and related processing of personal data;
8. types of prohibited Retaliatory Actions;
9. maintaining a register of Reports;
10. instructions on the options of reporting Legal Violations outside the inner channel.

§ 2

Terms used in the provisions of the Regulations:

Company – respectively, each of the companies within the Software Mind Group with its registered office in the territory of Europe, excluding those registered in Poland, in particular:

- Software Mind SRL (Moldova)
- Software Mind CF SRL (Romania)
- Software Mind, S.L. (Spain)
- Software Mind, GmbH (Germany)

Compliance Officer – a person designated within the Group, responsible for receiving Reports and authorised to take Subsequent Actions

Subsequent Actions – actions taken by the Company to assess the truthfulness of the information contained in the Report and, in appropriate cases, to prevent the Violation reported

Retaliatory Action – direct or indirect action or omission resulting from the Report that violates or may violate the rights of the Reporter or causes or may cause harm to the Reporter

Directive - Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

Software Mind, Group – Capital Group comprises 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

Violation Information – information, including a justified suspicion, concerning an actual or potential Violation that has occurred or is likely to occur within the Company, or information regarding an attempt to conceal such a Violation

Feedback – providing the Reporter with information about planned or taken Subsequent Actions and the reasons for such actions

Information Security Officer – a person responsible for managing information security within a given Company. In cases where no one in a given Company currently holds the position of Information Security Officer, the duties specified in the Regulations for a given violation may be performed by a designated member of the management body of that Company

Work-related context – past, present, or future actions related to the performance of work based on an employment relationship or other legal relationship constituting the basis for the provision of work or services or the performance of functions in or on behalf of a given Company, within which information about a Violation was obtained, and there is a possibility of experiencing retaliatory Actions

Violation – an action or omission defined in § 4 of the Regulations

Public Authority – a national authority designated in the country of the Company to receive external Reports and provide feedback to the Reporter or designated to fulfil other obligations related to legal violations and Subsequent Actions

Person Subject to the Report – a natural or legal person or organisational unit without legal personality, indicated in the Report or Public Disclosure as a person who committed the Violation or is associated with that person

Person Assisting in Making the Report – a natural person who assists the Reporter in making the Report or Public Disclosure in the work-related context

Person Associated with the Reporter – a natural person who may experience Retaliatory Actions in the work-related context, including a coworker or close person to the Reporter

Platform – an interactive electronic platform that allows Employees to make anonymous and confidential Applications related to illegal or unethical behaviour, available at the address indicated each time on the Company's website.

Employee – any person in an employment relationship with a given Company, regardless of the basis of their engagement, as well as any person cooperating with the Company on a basis other than an employment relationship

Public Disclosure – making information about a Violation public

Authorised – a person authorised to make a Report or Public Disclosure, as indicated in § 3 of the Regulations

Threat to life or health - a situation, or a suspected situation, that poses a real risk to an employee's life or health

Report – an internal Report or an external Report concerning a potential Violation that has occurred or is likely to occur

Internal Report – providing information about a Violation to the person responsible for receiving internal Reports in a given Company

External Report – providing information about a Violation to a Public Authority

Reporter – a person employed or cooperating with the Company, regardless of their position, function, form of employment or cooperation, or a participant in the recruitment or pre-employment negotiation process with the Company, or a person who maintains or has maintained contact with the Company in the work-related context, making a Report

§ 3

1. The Regulations apply to a natural person who reports or discloses Information about a Violation obtained in the work-related context, including:
    a. an employee,
    b. a person providing work on a basis other than an employment relationship, including under a civil law contract,
    c. a member of the Company's governing body,
2. Regardless of the authorized persons indicated in paragraph 1, the Rules apply to any natural person authorized to make a Report under the legislation of the country where the Company in which the Violation occurred has its registered office.

§ 4

1. A Violation is an action or omission that is contrary to the law or aims to circumvent the law concerning:
    a. Acts of the European Union concerning the following areas:
        - public procurement;
        - services, products, and financial markets;
        - preventing money laundering and terrorist financing;
        - product safety and compliance with requirements;
        - environmental protection;
        - consumer protection;
        - privacy and personal data protection;
        - the security of networks and information systems;
        - the financial interests of the European Union;
    b. the internal market of the European Union
    c. legal acts specified in the laws implementing the Directive in the countries where the respective Company has its registered office.

2. Additionally, the subject of an Internal Report may also include:
    a. improper performance of employment duties, resulting from applicable legal provisions and internal regulations within the Group and the relevant Company;
    b. unethical behaviours and actions, especially a violation of the Business Ethics Code applicable in the Software Mind Group;
    c. actions leading to that could lead to to a threat to the lives and health of employees and individuals cooperating with the Company on a different legal basis, violating occupational safety and health principles;

d. a suspected or actual threat to the life or health of employees that is not directly related to the work performed or to occupational health and safety regulations;
e. neglect of the well-being of the Company or Group and entrusted property, actions harmful to the Company or Group;
f. behaviour that violates applicable legal provisions.

§ 5

1. Every Employee is required to familiarise themselves with the content of the Regulations.
2. The obligation mentioned in paragraph 1 applies to all Employees, regardless of their position, working hours, and type of work performed.
3. The obligation mentioned in paragraphs 1 applies appropriately to other Authorised persons.

§ 6

1. Every Authorised person who has knowledge of a Violation while performing work, service, or in the provision of services to the Company should promptly make a Report indicating the circumstances of the situation.
2. The Company ensures impartiality in the verification of Reports and guarantees confidentiality and protection to Reporters, persons assisting in making a Report, as well as persons associated with the Reporter.

Chapter II

Procedure for Reporting Violations

§ 7

1. The Company has implemented an internal Reporting channel allowing for the submission of Reports in written form, through an interactive electronic Platform.
2. The Platform enables the submission of Reports confidentially and, if desired, anonymously by the Reporter.

3. Any Authorised person can submit Reports through the Platform.
4. The Authorised entity within the Group to receive Reports is the Compliance Officer.
5. If the Report relates to a Compliance Officer, the Report can be made using e-mail address of the Board Member of the Company to which the Report relates.
6. The Reporting Channels specified in the Rules do not exclude the possibility of submitting a Report in another form if such a form is provided for by the legislation of the country where the Company to which the Report relates has its registered office.

§ 8

1. Reports can be submitted through the Platform, available at the internet address indicated on the Company's website.
2. To submit a Report, one must complete the data specified in the Report form available on the Platform, including:
    a. specifying the company involved in the Violation,
    b. specifying the nature of the Violation,
    c. indicating the date of the Violation,
    d. specifying the location of the Violation,
    e. indicating individuals or groups of individuals involved in the Violation or affected by the Violation,
    f. describing the details of the Violation.
3. A report can be made confidentially or fully anonymously by selecting the appropriate option in the form.
4. Optionally, the Reporter may provide their personal data in the Report, such as: first name, last name, mailing address (i.e., street, house number, postal code, city, country), and indicate whether the Reporter is an employee of the company where the Violation occurred, which is the subject of the Report.
5. Additionally, the Reporter may provide their email address in the Report to receive notifications about the current processing status of the Report. If the Reporter does not provide an email address, they will not receive notifications about the current processing status of the Report but will have the opportunity to check the status of the Report through the login area mentioned in paragraph 8 below.
6. Providing the information mentioned in paragraph 3 above is not mandatory, but not providing the information may affect the effectiveness of Subsequent Actions, especially in conducting explanatory proceedings concerning the Violation.

7. Additional documents documenting the Violation can be attached to the Report, and a voice message regarding the Violation can be recorded.
8. After submitting the Report, the Platform will automatically generate individual login credentials (username and password) for the Reporter, allowing access to the login area. Through this area, the Reporter can check the processing status of the Report, contact the Compliance Officer, and provide further information regarding the Violation.
9. The Reporter should remember the received login credentials to maintain access to the login area on the Platform.
10. It is recommended that the Whistleblower refrain from public discussions about the reported violations and not disclose information related to the report to unauthorized persons, unless required by law. This recommendation is made solely to enhance the effectiveness of the investigative proceedings.

§ 9

1. The Company is obligated to:
    a. provide every Reporter with simple and anonymous access to the person responsible for receiving Reports,
    b. prevent unauthorized persons from accessing information covered by the Report,
    c. ensure protection for the Reporter against retaliatory Action,
    d. respect and protect the confidentiality of the Reporter's identity, the person concerned by the Report, and any third party mentioned in the Report,
    e. ensure the correctness of the processing of the Reporter's personal data in connection with the submitted Report,
    f. provide appropriate authorization to persons responsible for receiving Reports.
2. The Company offers employees the opportunity to use free, anonymous psychological consultations, particularly in the case of an internal report as referred to in paragraph 4 point 2c-d. Participation in the consultation is voluntary and does not affect job performance evaluations or any other HR decisions.
3. The Compliance Officer informs the Information Security Officer if the Report concerns the security of the Company's information and/or personal data, about the receipt of the reported Violation without disclosing the identity of the Reporter. The Information Security Officer is not informed if the matter may directly concern them.

4. If the reported Violation concerns the Compliance Officer or Information Security Officer, then actions in accordance with these Regulations are taken by a designated member of the Company's management body, excluding the respective Compliance Officer or Information Security Officer.

§ 10

1. A Report may, in any case, also be submitted directly to a public authority, bypassing the procedure set out in the Rules, in accordance with the legislation of the country where the Company to which the Report relates has its registered office.

Chapter III

Subsequent Actions

§ 11

1. The entity authorised at the Group level to take Subsequent Actions is the Compliance Officer. If the matter concerns the Compliance Officer, the internal entity authorised to take Subsequent Actions is a designated member of the management body of the Company to which the Report relates. In such a case, wherever the Regulations refer to the Compliance Officer, it should be understood as the designated member of the management body of the Company to which the Report relates.
2. The Compliance Officer is obligated to confirm this fact to the Reporter within 7 days of receiving the Report, through the Reporting Platform.
3. The Compliance Officer, along with the confirmation of receiving the Report, informs the Reporter of their rights and obligations arising from these Regulations and the further stages of reviewing their Report. This information includes provisions regarding the confidentiality and anonymity of the received Report.

§ 12

1. The Compliance Officer performs tasks ensuring the smooth functioning of the system to counter Violations, in particular by:
    a. maintaining a register of Reports,
    b. ensuring the review of each Report, i.e., conducting explanatory proceedings and, in justified cases, establishing teams whose composition enables a comprehensive clarification of the matter, and, in cases where the Employee expresses a willingness and need to receive psychological consultation – coordinating the process of arranging such consultation.
    c. fulfilling the information obligation towards the Reporter, in particular providing Feedback,
    d. ensuring the confidentiality of the Reporter's identity and information covered by the Report
    e. ensuring impartiality during the conducted explanatory proceedings,
    f. conducting informational campaigns among the Authorised Persons aimed at reinforcing a positive perception of actions related to Reports and promoting a responsible attitude,
    g. presenting the Company with the results of the explanatory proceedings and, in the event of a Violation, indicating the persons responsible for the Violation and proposing consequences for these individuals.
2. After receiving a Report, the Compliance Officer takes Subsequent Actions without undue delay.
3. Subsequent Actions include, in particular, the following activities:
    a. assessing the accuracy of the information contained in the Report,
    b. verifying information about the Violation, which includes determining the circumstances of the Violation and the identities of the persons who committed the Violation;
    c. full explanatory proceedings.
4. As part of Subsequent Actions, the Compliance Officer may take measures to verify information about the Violation, i.a. such as:
    a. continuing communication with the Reporter, including requesting additional information,
    b. obtaining explanations to establish the facts related to the Violation,
    c. requesting the issuance of copies or access to documents related to the Violation.
5. The Compliance Officer is obligated to take actions with due diligence.
6. For each action taken as part of the explanatory proceedings, the Compliance Officer prepares an official note, and in the case of receiving explanations, a conversation protocol. These documents are attached to the final report of the explanatory proceedings.
7. The actions referred to in paragraphs 3 a and b should be carried out jointly with the Information Security Officer if the Report concerns the information security

and/or personal data of the Company (excluding situations where the Report concerns the Information Security Officer) and aims to verify the accuracy of the received Report, including the grounds for taking action within the framework of a full investigation.

§ 13

1. If the initial explanatory proceedings have shown the justification for further actions by the Compliance Officer, together with the Information Security Officer if the Report concerns the security of information and/or personal data of the Company, they conduct a full explanatory proceeding involving additional verification of the Report.
2. As part of the full explanatory proceeding, the Compliance Officer, together with the Information Security Officer (if required by the subject of the Report and the Report does not concern the Information Security Officer), receives explanations from persons suspected of the Violation, witnesses of the Violation, and Reporters.
3. After completing the full explanatory proceeding, the Compliance Officer, together with the Information Security Officer (if he participated in the explanatory proceeding), prepares a report containing information on the results of the explanatory proceeding, including findings regarding the accuracy of the information in the Report and stating the occurrence or absence of a Violation, and submits it to the management body of the Company. If the explanatory proceeding concerned the actions of a member of the management body of the Company, the report is presented to the supervisory body of the Company.
4. If the report from the initial and/or full explanatory proceeding finds the occurrence of a Violation, the management body of the Company takes consequences against persons who committed the Violation, and also, if required by the regulations of the applicable law, reports the Violation to the relevant authorities. If a member of the management body of the Company committed the Violation, the actions mentioned in this point are taken by the supervisory body of the Company.

§ 14

1. Within the time frame specified in the law implementing the Directive in the country where the Company to which the Report relates has its registered office, Compliance Officer provides the Reporter with feedback through the

login area on the Platform and simultaneously through an email notification, unless the Reporter has not provided their email address in the Report.

2. As a result of the conducted Follow-up Actions, the Report may be considered:
    a. Valid, and corrective actions and/or consequences are taken.
    b. Unfounded (not confirmed), and the Report is dismissed.
3. Regarding a person who committed a Violation, the Company may apply consequences provided by the law, especially:
    a. Apply disciplinary consequences, including a reprimand or warning;
    b. Change employment conditions, including assigning different duties;
    c. Terminate the employment relationship;
    d. Terminate a civil law contract;
    e. Take other actions provided by the law, including reporting the Violation to the relevant authorities.

Chapter IV

Protection of the Reporter of a Violation

§ 15

1. Personal data of the Reporter and other information allowing the determination of their identity shall not be disclosed to unauthorised persons unless expressly agreed by the Reporter.
2. The provisions of paragraph 1 do not apply when the obligation to disclose the personal data of the Reporter to the competent public authorities or courts arises from the provisions of the applicable law. Personal data collected in connection with the acceptance of the Report and conducting Follow-up Actions are processed by the Company in accordance with the principles specified in Chapter V of these Regulations.
3. The provisions of points 1–3 also apply to the Person assisting in making the Report, the Person associated with the Reporter, and the Person to whom the Report pertains.

§ 16

1. The company will not take any retaliatory actions or attempt or threaten to take such actions against the reporting party, nor will it treat the reporting party unfavourably due to making an internal or external report.

2. In the case where the reporting party is an employee, retaliatory actions referred to in point 1 shall include, in particular:
    a. suspension, forced unpaid leave, dismissal;
    b. demotion or suspension of promotion;
    c. reassignment of duties, change of workplace, reduction in salary, change of working hours;
    d. suspension of training;
    e. negative performance evaluation or negative opinion about work;
    f. imposition or application of any disciplinary measure, reprimand, or other punishment, including financial penalties;
    g. coercion, intimidation, mobbing, or exclusion;
    h. discrimination, unfavorable or unfair treatment;
    i. failure to convert a fixed-term employment contract into an indefinite-term employment contract when the employee could have had a reasonable expectation of being offered permanent employment;
    j. failure to extend or early termination of a fixed-term employment contract;
    k. referral for psychiatric or medical examinations.
3. The provisions of Point 2 apply accordingly if work, services, or works were, are, or are to be performed for the company on the basis of a legal relationship other than an employment relationship, constituting the basis for the provision of work, services, performance of works, or the performance of functions.
4. Each reporting party who has become the target of retaliatory actions or suspects that they may become the target of retaliatory actions should report this fact to the compliance officer.
5. An exception to the rule of maintaining the confidentiality of the identity of the reporting party and information about the violation arises when the law requires the company to disclose information about the violation or the Whistleblower consents to the disclosure of their identity.
6. The reporting party is subject to protection specified in this chapter under the condition that at the time of making the report, they had reasonable grounds to believe that the information subject to the report is true and constitutes information about a violation (report made in good faith).
7. The rights and protection provided for in this regulation do not apply to the reporting party who, when making the report, did not act in good faith, in particular, made a conscious report of false information. In such a case, the reporting party may be subject to disciplinary action and also legal liability under applicable laws.

Chapter V

Principles of Personal Data Protection

§ 17

1. The controller of the personal data collected and processed in connection with the submission of a report and the implementation of Subsequent Actions is the Company where the report was made.
2. In all matters related to the processing of personal data in connection with the consideration of the report, especially regarding the exercise of rights related to their processing, the reporting party may contact the Company via email at personal.data@softwaremind.com or in writing at the correspondence address of the administrator.
3. The Company provides information on its website and on the platform designated for making reports about the principles of processing personal data in connection with the acceptance of reports and the implementation of Subsequent Actions, in accordance with the requirements arising from the relevant data protection regulations.

§ 18

1. The process of accepting and verifying reports, implementing Subsequent Actions, and the associated processing of personal data should be organised in a way that prevents unauthorised access to the information covered by the report and ensures the confidentiality of the identity of the reporting party, the person the report concerns, and third parties indicated in the report. The confidentiality protection applies to information that can directly or indirectly provide the identity of such persons.
2. Persons authorised to accept and verify reports, implement Subsequent Actions, and process personal data in connection with the consideration of the report are obligated to maintain absolute confidentiality regarding all facts learned during these activities and in connection with them. Before taking any action, they are required to sign a declaration of the obligation to maintain absolute confidentiality of this information.
3. At the same time, the persons referred to in paragraph 2 receive written authorisation from the Company to take actions related to accepting and verifying reports, implementing Subsequent Actions, and processing personal data in connection with the consideration of the report.

4. The Company ensures, in particular, training for the Compliance Officer and Information Security Officer regarding the obligation to maintain the confidentiality of information to which they have access in connection with the performance of duties covered by this Regulation.
5. The platform used by the Company for making reports ensures secure and compliant processing of personal data related to a given report, including the personal data of the reporting party and the person the report concerns.
6. All information and documents collected in connection with the consideration of the report should be stored with appropriate security measures to prevent unauthorised access to their content.

§ 19

Every report submitted in accordance with the Regulation, along with data concerning the reporting party or data enabling their identification, is confidential.

§ 20

1. Personal data processed in connection with the submission of a Report or the undertaking of Subsequent Actions, as well as documents related to the Report or Subsequent Actions, constitute confidential information and are stored by the Company for the period specified in the law implementing the Directive, in the country where the Company to which the Report relates has its registered office.
2. The Company deletes personal data and destroys documents related to a specific Report after the storage period has expired, as specified in paragraph 1. Personal data that are not relevant to the handling of the Report are not collected, and if collected by mistake, they are immediately deleted.

Chapter VI

Report Register

§ 21

1. The Company maintains a register of all information received based on this Regulation. The register includes, in particular, the report number, the subject of the legal violation, the personal data of the whistleblower and the person to whom the report pertains, the contact address of the whistleblower, the date of the report, information on subsequent actions taken, and the date of case closure.
2. The responsibility for maintaining the register is entrusted to the Compliance Officer. The Register of Reports concerning the Compliance Officer is kept separately by a member of the Company's management body, excluding the Compliance Officer.
3. All documents received from reporters, as well as the information indicated in paragraph 1 above, must be classified and treated as confidential, following the applicable information security policy.

Chapter VII

Final Provisions

§ 22

1. The Company ensures that every new Employee and other Authorised persons are informed about the applicable Regulation, its content, and the channels for reporting Violations.
2. The management body of the Company may develop an internal instruction regulating the details of the procedure for accepting Reports, conducting preliminary and full explanatory proceedings, and reporting identified Violations to the relevant public authorities. In case of any discrepancies between the content of this Regulation and the content of the developed instruction, the relevant provisions of the Regulation shall take precedence.

§ 23

1. In matters not regulated by this Regulation, the provisions of universally applicable law apply, in particular the relevant provisions of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23 2019, on the protection of persons reporting breaches of Union law, as well as the provisions of the legislation of the country where the Company to which the Report relates has its registered office.
2. In the case of discrepancies between the provisions of this Policy and the legislation of the countries where the Companies have their registered offices, the provisions of the national legislation shall take precedence.