

Internal Reporting Regulations Defining Procedures for Reporting Irregularities and Protecting Whistleblowers

§ 1. Purpose of the Regulations

1. The purpose of these Regulations is, in particular, to define:
 - a. violations of law subject to reporting under these Regulations;
 - b. persons authorized to submit internal reports;
 - c. principles for receiving and processing internal reports, including follow-up actions;
 - d. roles, tasks, and responsibilities of participants;
 - e. rules for maintaining the confidentiality of the identity of authorized individuals;
 - f. protection of authorized persons from retaliatory actions.
2. The principles contained in these Regulations do not infringe upon or limit the obligation to notify the appropriate state authorities in accordance with their competencies, especially in cases of reasonable suspicion of a crime.

§ 2. Definitions

1. Whenever these Regulations refer to:
 - a. **follow-up action** – this means actions taken by the employer or public authority to assess the validity of allegations in the report and, where applicable, to prevent violations of law subject to the report, including through internal investigations, explanatory proceedings, filing charges, actions to recover funds, or closing the reporting and verification procedure;

- b. **retaliatory action** – this means direct or indirect action or omission resulting from the report or public disclosure, which violates or may violate the rights of the whistleblower or causes or may cause harm to the whistleblower;
- c. **information on a violation of law** – this means information, including reasonable suspicion, about an actual or potential violation of law that occurred or is likely to occur within the organization where the whistleblower works or worked, or in another organization with which the whistleblower has or had work-related contact, or information about an attempt to conceal such a violation;
- d. **feedback** – this means providing the whistleblower with information about planned or undertaken follow-up actions and the reasons for those actions;
- e. **work-related context** – this means all circumstances related to an employment relationship, service, or other legal relationship forming the basis for the provision of work, through which information about a violation of law was obtained;
- f. **central authority** – this means a public administration body responsible for providing information and support regarding reporting and public disclosure of violations of law and for receiving external reports of violations in areas covered by the Act, their preliminary verification, and referral to competent authorities for follow-up actions;
- g. **public authority** – this means a public administration body that has established procedures for receiving external reports of violations of law within the scope of its activities;
- h. **person subject to the report** – this means a natural person, legal entity, or organizational unit without legal personality but granted legal capacity by law, indicated in the report or public disclosure as a person who committed the violation or is associated with such a person;
- i. **person assisting with the report** – this means a natural person who assists the whistleblower in making a report or public disclosure in a work-related context;

- j. **person related to the whistleblower** – this means a natural person who may experience retaliatory actions, including a coworker or a family member of the whistleblower;
- k. **employer** – this means an employer as defined in the Labor Code (Journal of Laws 2023, item 1465, Article 3) or a principal as defined in the Civil Code;
- l. **employee** – this means an employee as defined in the Labor Code (Journal of Laws 2023, item 1465, Article 2) or a contractor as defined in the Civil Code;
- m. **public disclosure** – this means making information about a violation of law available to the public;
- n. **report** – this means an internal or external report;
- o. **internal report** – this means providing information about a violation of law to the employer;
- p. **external report** – this means providing information about a violation of law to a public authority or central authority;
- q. **authorized person** – this means an employee or employees authorized by the employer to receive and verify internal reports, take follow-up actions, and process personal data of individuals mentioned in the internal report;
- r. **team** – this means a team consisting of authorized persons;
- s. **Directive** – this refers to Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, on the protection of persons who report breaches of Union law (OJ EU L 305, p. 17);
- t. **Act** – this refers to the Act of June 14, 2024, on the Protection of Whistleblowers (Journal of Laws 2024, item 928);
- u. **GDPR** – this refers to Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ EU L 119, p. 1, as amended).

§ 3. Scope of the Regulation: Subject Matter and Entities

1. The subject of the report may include information about violations of the law, consisting of actions or omissions contrary to the law or intended to circumvent the law, concerning:
 - a. public procurement;
 - b. financial services, products, and markets;
 - c. prevention of money laundering and terrorist financing;
 - d. product safety and compliance;
 - e. transport safety;
 - f. environmental protection;
 - g. radiological protection and nuclear safety;
 - h. food and feed safety;
 - i. health and animal welfare;
 - j. public health;
 - k. consumer protection;
 - l. privacy and personal data protection;
 - m. network and information system security;
 - n. the financial interests of the European Union;
 - o. the internal market of the European Union, including competition and state aid rules and corporate taxation.

§ 4. Persons Authorized to Make Reports

1. Persons authorized to make internal reports, in the context of work, are:
 - a. employees;
 - b. individuals whose employment relationship has been terminated;
 - c. job candidates participating in the recruitment process before the conclusion of an agreement.
2. The provisions of this Regulation also apply appropriately to persons assisting the reporter in making an internal report.

§ 5. Circumstances Excluding the Application of the Regulation

1. The provisions of this Regulation do not apply if:

- a. the internal report was not made in the context of work, or the person acted in bad faith;
- b. the information about the violation of the law does not concern public interest or a broader group of individuals but relates exclusively to the interests or rights of the reporter;
- c. the report was made by the perpetrator of the violation who derives favorable legal consequences for themselves due to the internal report.

§ 6. Entities (Persons) Authorized to Receive Internal Reports and Take Follow-Up Actions

1. The entity authorized by the employer to receive internal reports includes:
 - a. employees authorized by the employer.
2. The entity authorized to consider reports and take follow-up actions, including verifying the report and further communication with the reporter (e.g., requesting additional information and providing feedback), is the Internal Reporting Team.
3. The Internal Reporting Team consists of individuals designated to handle specific reports.
4. In carrying out the tasks within this scope, authorized individuals are required to treat all reports with due seriousness and care, ensuring confidentiality. When considering reports, they must adhere to principles of impartiality and objectivity.
5. The aforementioned employees perform the tasks specified in the Regulation based on authorization from the employer.

§ 7. Making Internal Reports and Rules for Receiving Them

1. Internal reports can be made:
 - a. Electronically, via the email address **speakup@simplycontact.com**, which is dedicated solely to handling reports about violations and is not used for the entity's ordinary activities;
 - b. Electronically, through a form available on the website **simplycontact.com** or directly via the link <https://simplycontact.peopleforce.io/speak/8v9m0v4k>;

- c. Electronically, through a form available on the main page of the employee platform **PeopleForce**.
2. The internal report should include, in particular:
 - a. If the report is not anonymous – the reporter’s details: full name, position, and contact details (postal address or email address);
 - b. Date and place of the internal report’s submission;
 - c. Information about the person(s) who committed the violation, including their full name, position, and workplace;
 - d. A description of the violation, including the date, location, and circumstances of the incident;
 - e. Whether the reporter consents to the disclosure of their identity.
3. The reporter may attach evidence supporting the described violation to the internal report, as well as a list of witnesses to the described violation.
4. A template for the internal reporting form is provided in Annex 1 to the Regulation.

§ 8. Registration and Consideration of Reports

1. Upon receipt of an internal report, the authorized person registers the report and forwards it to designated members of the Internal Reporting Review Team.
2. The Internal Reporting Review Team is appointed by the Employer or a designated Employee.
3. The Team conducts a preliminary formal verification to determine whether the report pertains to a legal violation within the scope of the authority's activities. If not, the appropriate public authority for follow-up actions is identified.
4. If the authority is found not to have jurisdiction to consider the report, the Team forwards the internal report without delay—no later than 14 days from the report's receipt, or within 30 days in justified cases—to the competent public authority and informs the whistleblower accordingly.
5. If the report pertains to violations within the authority's scope, the Team considers the report and takes follow-up actions with due diligence.
6. If additional information is required to process the internal report, the Team may contact the whistleblower at any stage using the provided contact details.

7. The Team provides feedback to the whistleblower no later than three months after the internal report's receipt.
8. In justified cases, feedback may be provided within six months, with prior notice to the whistleblower before the three-month deadline specified in point 7.
9. At the request of the person authorized to handle reports, every employee is required to provide necessary information or make requested documents available to establish the circumstances of the internal report.
10. Employees must cooperate as necessary during the investigation, including providing information and appearing at specified times for interviews.
11. The authorized person is responsible for collecting documents necessary to verify the report's validity and records actions in official notes.
12. A protocol is prepared during interviews with employees summoned for explanations.
13. All participants in the investigation must maintain confidentiality regarding any information obtained, even after the investigation concludes.
14. Following verification of the report's validity and the accuracy of the information about the legal violation, the investigation concludes with a final report:
 1. confirming the validity of the information;
 2. rejecting the validity of the information.
15. The final report includes a description of the legal violation, findings of the investigation, the validity of the report, and, if valid, recommendations for actions regarding the person involved and measures to prevent similar violations in the future.
16. After reviewing the final report, the employer decides on measures to address identified violations and prevent recurrence, including employment law actions, organizational changes, control activities, or notifying the competent authorities.

§ 9. Data Protection, Confidentiality, and Document Handling

1. The personal data of the whistleblower and the person implicated are protected under personal data protection laws.
2. The whistleblower's personal data and identity are not disclosed without explicit consent, except as required by law.

3. The whistleblower must be informed whenever disclosure of their identity becomes necessary, such as during criminal proceedings.
4. Documentation resulting from an internal report:
 - a. cannot be shared or disseminated except as legally required;
 - b. is protected under personal data laws, especially if it could reveal the whistleblower's or implicated person's identity;
 - c. is stored in compliance with the data retention period specified by whistleblower protection laws.

§ 10. Retaliatory Actions

1. Retaliation against a whistleblower protected under this Regulation is strictly prohibited. This includes threats or attempts to retaliate.
2. Prohibited forms of retaliation include but are not limited to:
 - a. refusal to establish an employment relationship;
 - b. termination of employment, with or without notice;
 - c. refusal to extend or renew fixed-term contracts when there is a reasonable expectation of renewal;
 - d. reduction of salary;
 - e. withholding promotion or exclusion from advancement opportunities;
 - f. exclusion from employment-related benefits;
 - g. demotion or reassignment to a lower position;
 - h. suspension from duties;
 - i. reassignment of duties;
 - j. changes to the place or schedule of work to the employee's disadvantage;
 - k. negative performance evaluations or opinions;
 - l. disciplinary actions, including financial penalties;
 - m. exclusion from training opportunities for professional development;
 - n. unjustified referrals for medical or psychiatric evaluations;
 - o. actions impeding future employment in the sector or industry.

Retaliation is only permissible if the employer proves it was based on objective reasons.

§ 11. Protection of Whistleblowers

1. A whistleblower is entitled to protection provided they had reasonable grounds to believe that the reported information about a legal violation was accurate at the time of submission and that the information constitutes a report of a legal violation, regardless of whether the violation was ultimately confirmed during the proceedings.
2. The provisions of § 17 section 2 apply to individuals assisting in making the report and those associated with the whistleblower, provided they are also employed by the employer of the whistleblower.
3. Confirmed retaliatory actions against a whistleblower in connection with their report constitute a breach of employee duties and may result in disciplinary and legal consequences under applicable laws.
4. To ensure protection against retaliation, employees authorized to handle whistleblower reports monitor the employment situation of the whistleblower.
5. Measures to protect whistleblowers include:
 - a. Restricting access to information solely to authorized individuals as part of the investigation and the process of protecting the whistleblower and anyone assisting them.
 - b. Obtaining written confidentiality agreements from those authorized to access the information during the investigation or the whistleblower protection process.
 - c. Disciplining individuals found to have violated confidentiality agreements under applicable disciplinary regulations.
6. Whistleblowers must be informed of circumstances under which their identity may need to be disclosed, such as in the event of criminal proceedings.

§ 12. Right to External Reporting

1. A report may also be made directly to a public authority or central agency, bypassing the internal reporting procedures outlined in these regulations, especially if:
 - a. The employer fails to take follow-up actions or does not provide feedback within the mandated 7-day period.

- b. The whistleblower has reasonable grounds to believe that the violation poses an immediate or clear threat to public interest, such as the risk of irreversible damage.
 - c. Making an internal report would expose the whistleblower to retaliation.
 - d. The circumstances of the case suggest that internal reporting is unlikely to effectively address the violation, e.g., evidence may be destroyed or hidden, or collusion may exist between the employer and the violator.
2. External reporting does not negate statutory protections for whistleblowers.

§ 13. Public Disclosure

1. Whistleblowers making a public disclosure are protected if:
 - a. They first made an internal and then an external report, but no appropriate follow-up action or feedback was provided within the prescribed timeframe.
 - b. They reported externally, but the public authority failed to act or provide feedback within the designated timeframe.
2. The above requirements do not apply if the whistleblower has reasonable grounds to believe that:
 - a. The violation poses an immediate or clear threat to public interest, such as the risk of irreversible harm.
 - b. External reporting would expose them to retaliation.
 - c. External reporting is unlikely to effectively address the violation due to circumstances such as collusion or involvement of the public authority in the violation.
3. Sections 1 and 2 of § 20 do not apply if the information is directly provided to the press in accordance with Art. 15 section 2 point 1 of the Press Law Act of January 26, 1984 (Journal of Laws of 2018, item 1914).

§ 14. Final Provisions

1. These regulations are reviewed at least once every three years.
2. The regulations are published on the simplycontact.com website and the PeopleForce employee system.

3. Simply Contact LLC prepares an annual statistical report on the number of reports received and their outcomes by March 31 of the following year.
4. Attachments to these regulations include:
 - a. Attachment 1: Template for Reporting Irregularities/Violations.
 - b. Attachment 2: Template for Internal Reporting Register.

Attachment 1 to the Internal Reporting Regulations

Template for Reporting Irregularities/Violations

I. Legal Basis

Order No. 1/2024, dated December 19, 2024

II. Reporting Person

Name and surname:

(In the case of a report submitted by several persons, please include all their names.)

III. Contact Information

Name and surname:

Job position:

Phone number or email:

IV. Person Concerned by the Report

Name and surname:

(In the case of a report concerning several persons, please include all their names.)

V. Description of Events

(Provide a detailed description of the events or occurrences indicating suspected undesirable behavior as defined in the regulations. Describe each undesirable event, its date, and any potential consequences. You may also include any available evidence, such as documents, email correspondence, or witness details.)

VI. Attachments to the Report *Include any evidence in the form of attachments.*

.....

.....

(Date and signature of the reporting person)

VII. Consent to Disclosure of Identity

Yes..... No

