



a coesia company

FlexLink Systems SP. Z O.O. Poland Whistleblowing Policy

Contents

Part A - GLOBAL WHISTELBLOWING POLICY	3
1. Purpose	4
2. Who can report violations	4
3. What can and cannot be reported at the global level	4
4. How to report	5
Part B - LOCAL INTERNAL REPORTING PROCEDURE	6
1. Scope	7
2. Violations of the law	8
3. Entity authorized to receive reports	9
4. Internal reporting channels	10
5. Reporting	11
6. Confidentiality of the report	12
7. Follow-up	13
8. Handling the report	13
9. Submission to global structures	15
10. External application	15
11. Protection of whistleblowers	15
12. Disabling protection	16
13. Familiarizing the Employee with the content of the Procedure	17
14. Applicable law and Final Provisions	17

Szkolna 30, 62-064 Plewiska, entered into the Register of Entrepreneurs of the National Court Register kept by the District Court Poznań – Nowe Miasto and Wilda in Poznań, VIII Commercial Division of the National Court Register under KRS 0000082639, having REGON 639711806, NIP 7822142445, share capital: PLN 480,500.00, BDO number: 000009443, (hereinafter also referred to as: “**FlexLink**” or “**Employer**”)

FlexLink is part of the Coesia Group. This document regulates the rules for whistleblowing both at the global level (section one) and at the national level (Poland), as part of the internal whistleblowing system (section two).

A.
GLOBAL
WHISTELBLOWING
POLICY
(Global level)

The following rules apply to reports made in accordance with the Global Whistleblowing Policy of the Coesia Group, to which FlexLink belongs.

The Policy on the national internal whistleblowing system (level of Polish legislation) is set out below in Section II.

Whistleblowers need to submit their report through the digital platform NAVEX where they can choose whether to address their report at Coesia Group level or locally at FlexLink.

1. Purpose

- 1.1 In particular, the purpose of the Global Whistleblowing Policy is to provide all individuals acting on behalf of, for or for or in the interest of Coesia S.p.A. (including FlexLink as its subsidiary) with an operational tool to report violations of the Coesia Code of Ethics, of Coesia Policies, as well as all applicable national and international laws in force in the countries where Coesia companies operate¹.

2. Who can report violations

- 2.1 Anyone can submit a report. Coesia S.p.A. and FlexLink, as a subsidiary, extend the possibility of reporting irregularities to all persons who, in the context of their professional activity, become aware of a possible violation

3. What can and cannot be reported at the global level

- 3.1 Anyone can make a report if they find any suspicion or violation of:
- Coesia Code of Ethics;
 - Coesia policies or procedures;
 - Including national laws and regulations².

¹ With the exception of certain provisions of Polish law and other regulations referred to in Part Two of this Policy, i.e. the Local Internal Reporting Procedure (level of Polish legislation).

² With the exception of certain provisions of Polish law and other regulations referred to in Part Two of this Policy, i.e. the Local Internal Reporting Procedure (level of Polish legislation).

- 3.2 You can't report violations based on information obtained solely on the basis of unreliable speculation or rumours.

4. How to report

- 4.1 Submission channels at the global level:

WRITTEN FORM

Through a digital reporting platform available online via:

- computer at the following link: **coesia.ethicspoint.com**;
- mobile phone at **coesia.navexone.eu** or by scanning the **QR code**:



ORAL FORM

- toll-free numbers³ are available on the **coesia.ethicspoint.com** portal (24 hours a day – 7 days a week)

- 4.2 Once you have submitted your report, you will receive an access code called a "report key" which, along with your password, can be used to check your answers or questions on the platform.

- 4.2 **Anonymity and Confidentiality**

Whistleblowers can report breaches:

- **Openly:** Applicants provide their full personal details and contact details;
- **Anonymously:** The Reporter may choose to provide his/her contact email address through the NAVEX platform, which will not be transferred to FlexLink Systems Sp. z o.o. or Coesia or any of their companies, but will allow you to receive notification emails when an answer or question is published in the system or the Reporter can remain completely anonymous. In this case, it will be up to the Submitter to use their password and 'report key' to access the system to check the feedback.

For more information on global reporting, please refer to Coesia's Global Whistleblowing Policy.

³ The hotlines are managed by employees of Navex (the digital platform chosen by Coesia S.p.A., which complies with international regulatory requirements and guarantees the highest standards of security and data protection: all processing of sensitive personal data will be carried out in full compliance with current regulations), who transcribe the report into the system.

B.
LOCAL INTERNAL
REPORTING
PROCEDURE
(level of
Polish legislation).

*The following procedure (hereinafter referred to as the “**Procedure**”) governs the internal whistleblowing system established in accordance with Polish legislation⁴. The rules for notification at the global level are set out above in section “I. Global policy on whistleblowing (Global level)”.*

1. Scope

- 1.1 This Procedure sets out the internal rules for reporting breaches of the law, potential or existing at the Employer’s premises, and for the Employer to take follow-up actions, as well as the conditions for covering the protection of persons reporting breaches of the law and persons associated with them.
- 1.2 In accordance with the Procedure, persons who report information about a violation of the law, obtained in a work-related context, are entitled to submit internal reports, including:
1. employee;
 2. temporary worker;
 3. a person performing work on a basis other than an employment relationship, including on the basis of a civil law contract;
 4. entrepreneur;
 5. proxy;
 6. shareholder or partner;
 7. member of a body of a legal person or an organizational unit without legal personality;
 8. a person performing work under the supervision and direction of a contractor, subcontractor or supplier;
 9. trainee;
 10. volunteer;
 11. apprentice;
 12. a person who has obtained information about a violation of the law **before the establishment of an employment relationship** or other legal relationship constituting the basis for the provision of work, services or performance of functions for the Employer or for the Employer, as well as **after their termination**, (hereinafter jointly referred to as the “**Whistleblowers**”).

2. Violations of the law

- 2.1 Whistleblowers, bearing in mind the Employer's best interest and the protection of the public interest, should report breaches of the law that occurred with the Employer, as referred to in paragraphs 2 and 3 below.
- 2.2 A notice of a breach of law is any information, including a reasonable suspicion of an existing or potential breach of the law, which has occurred or is likely to occur at an Employer with whom the Whistleblower participated in the recruitment process or other pre-contractual negotiations, works or worked, or at another legal entity with which the Whistleblower maintains or has maintained contact in a work-related context, or information regarding an attempt to conceal such a violation of the law.
- 2.3 **An infringement of the law** is an act or omission that is unlawful or aimed at circumventing the law, concerning:
1. Corruption;
 2. Procurement;
 3. financial services, products and markets;
 4. counteracting money laundering and terrorist financing;
 5. product safety and compliance;
 6. transport safety;
 7. Environmental;
 8. radiation protection and nuclear safety;
 9. food and feed safety;
 10. animal health and welfare;
 11. public health;
 12. consumer protection;
 13. protection of privacy and personal data;
 14. security of networks and ICT systems;
 15. the financial interests of the State Treasury of the Republic of Poland, local government units and the European Union;
 16. the internal market of the European Union, including public law rules on competition and state aid, and corporate taxation;
 17. constitutional freedoms and rights of man and citizen – occurring in the relations of an individual with public authorities and not related to the areas indicated in points 1-16 above.

⁴ The procedure was adopted by FlexLink Systems sp. z o.o. pursuant to Article 24 of the Whistleblower Protection Act of June 14, 2024 (Journal of Laws of 2024, item 928 (hereinafter referred to as the "Act").

- 2.4 Whistleblowers may report breaches of the Employer's internal regulations or ethical standards, including the Coesia Code of Ethics and Coesia's anti-corruption policy and other policies.
- 2.5 Information about violations of the law other than those specified in sections 2 – 4 will not be recognized in the manner provided for in the Procedure and the Act.
- 2.6 Information about the violation of the law should be provided through the internal reporting channels referred to in Article 4 of the Procedure.

3. Entity authorized to receive reports


- 3.1 The persons authorized by the Employer to receive internal reports are the members of the **Whistleblowing Management Team**: two members of the Ethics Committee of Coesia S.p.A. Paolo Fabiani and Paola Lanzarini (or persons holding the same position in Coesia S.p.A.) and the other two members as local contact persons, i.e.: Katarzyna Kaczmarek, HR Business Partner and Joanna Brzustowska, Finance Manager or persons holding the same position in FlexLink Poland (constituting the so-called Local Reporting Management Team irregularities). Each member of the Whistleblowing Management Team may act independently in carrying out tasks specified in this Procedure.
- 3.2 Each member of the Local Whistleblowing Management Team individually is authorised to: receive and document reports, confirm receipt of the report, provide feedback to the Whistleblower, follow up and provide feedback to the Whistleblower.

4. Internal reporting channels

4.1 The Employer has the following internal channels for submitting reports:

WRITTEN FORM

Through a digital platform available online through:

- computer at the following link **coesia.ethicspoint.com**;
 - mobile phone at **coesia.navexone.eu** address or by scanning the **QR code**:
- 
- **Via e-mail** – by sending it to the HR Business Partner, a member of the Whistleblowing Management Team, at the following address: **katarzyna.kaczmarek@flexlink.com**
 - **In writing to the following address**: FlexLink Systems sp. z o.o. with its registered office in Plewiska, 30 Szkolna Street, 62-064 Plewiska, **with the note: “Informing about irregularities - in person”** with the data of the person authorized to receive reports;

ORAL FORM

- **By phone** - toll-free phone numbers are available on the **coesia.ethicspoint.com** portal (24 hours a day – 7 days a week);
- **In person** at the request of the Whistleblower - through a direct meeting requested by email: **katarzyna.kaczmarek@flexlink.com**;

4.2 An oral report made via a recorded telephone line or other recorded voice communication system is documented with the Whistleblower’s consent in the form of:

1. a searchable recording of the conversation, or
2. A complete and accurate transcript of the call by an entity authorized to receive reports.

4.3 An oral report made via an unrecorded telephone line or other unrecorded voice communication system is documented in the form of a protocol of the conversation, reconstructing its exact course by the entity authorized to receive reports.

4.4 Meeting with the Whistleblower referred to in section 1 point 2 subsection b) it should be organised within 14 days from the date of receipt of such a request. In such a case, with the consent of the Whistleblower, the report is documented in the form of: minutes of the meeting, reconstructing its exact course, prepared by a person authorized to receive reports.

- 4.5 The whistleblower can check, correct and approve the minutes of the meeting by signing it.
- 4.6 The identification data of the person responsible for receiving and handling reports submitted through the internal reporting system, including their contact details, are published on the Employer's website: <https://www.flexlink.com/en/about-us/business-ethics>. Only authorized persons have access to the phone line and email address, so that the Whistleblower's identity is protected.

5. Reporting

- 5.1 In order for the report to be effectively identified and followed, it is recommended that the report indicate:
- date and place of the occurrence of the irregularity or obtaining information about the irregularity;
 - description of the event;
 - indication of the person to whom the report relates;
 - indication of possible witnesses;
 - indication of other evidence that may be helpful in the examination of the report;
- 5.2 The whistleblower should sign the report with their name.
- 5.3 The report may contain other data on the basis of which the person authorised to receive reports can determine/infer the identity of the Whistleblower.
- 5.4 The whistleblower may provide contact details (correspondence address or e-mail address) for the purpose of providing feedback and further communication. Lack of contact details will prevent feedback and further communication with the Whistleblower.
- 5.5 **Anonymous reports are left unprocessed. In exceptional situations, justified by the circumstances of the case, the Employer may consider an anonymous report.**

- 5.6 An oral report is made by the Whistleblower by phone or by leaving a voice message on the appropriate telephone line referred to in Article 4(1)(2) of this Procedure. The whistleblower may send a Written Notice to the relevant e-mail address of persons authorized to receive reports or send it in paper form to persons authorized to receive reports. Such a written document must be labelled “*Whistleblowing*”. Documents marked “*Whistleblowing*” may only be opened by Persons authorized to receive reports, and not by another employee of the Employer or any other person other than the Authorized Persons.

6. Confidentiality of the report

- 6.1 The Whistleblower’s personal data and other data allowing to determine their identity **are not disclosed** to unauthorized persons, except with the express consent of the Whistleblower.
- 6.2 An exception to the above-mentioned confidentiality rule is where disclosure is a necessary and proportionate legal obligation in connection with investigations conducted by public authorities or preparatory or judicial proceedings conducted by courts, including to guarantee the rights of defense of the person concerned.
- 6.3 After receiving the report, the employer processes personal data to the extent necessary to accept the report or take any follow-up action. Personal data that is not relevant to the processing of the report will not be collected and will be deleted immediately in the event of accidental collection. Such personal data shall be erased within 14 days of establishing that they are irrelevant.
- 6.4 Information concerning or originating from the Whistleblower is confidential and confidential. The employer is obliged to protect the identity of the Whistleblower and all details of the report. Only authorized persons involved in processing reports have access to this data.

7. Follow-up

- 7.1 The local whistleblowing management team referred to in Article 3(2) of the Procedure is authorised to take follow-up actions, including verifying the report and further communication with the Whistleblower, including requesting additional information and providing feedback to the Whistleblower.
- 7.2 Follow-up actions are taken with due diligence by an authorised entity, respecting the dignity and good name of the persons concerned.
- 7.3 The employer ensures the impartiality of the verification of reports – all information contained in the report should be checked and objectively evaluated.
- 7.4 Reports of violations should be considered in the order in which they are received, unless the seriousness or nature of the violation in question speaks in favor of prioritizing a given case.

8. Handling the report

- 8.1 The local whistleblowing management team is obliged to **confirm to the Whistleblower that the report has been received within 7 days from the date of its receipt**, unless the Whistleblower has not provided a contact address to which the confirmation should be sent.

The local whistleblowing management team conducts follow-up activities to verify information about violations of the law and to assess the veracity of the allegations contained in the report. An internal investigation or a proper investigation can be carried out for this purpose

- 8.2 Within a period not exceeding 3 months from the confirmation of receipt of the report, the Local Whistleblowing Management Team is obliged to provide feedback to the Whistleblower. Feedback includes, in particular, information on whether or not a violation of the law has been found and any measures that have been or will be used in response to the violation of the law and the reasons for such actions.

- 8.3 If the report is assessed as unfounded, the Whistleblower shall be notified without undue delay that no violation has been identified on the basis of the circumstances indicated in the Report or on the basis of the documents submitted by the Whistleblower and the actions taken, and the Whistleblower shall be instructed of the right to file a report with a public authority. The procedure for recognizing this report at the Employer is closed.
- 8.4 If the report is assessed as justified, the persons examining the report will propose to the Employer measures to prevent or correct the illegal situation.
- 8.5 If a violation of the law is found, follow-up actions may include, m.in others, reporting a crime or misdemeanor, bringing prosecution, actions aimed at recovering funds, initiating inspections, administrative proceedings, professional or disciplinary consequences against the perpetrator of the violation.
- 8.6 If you are part of the Local Whistleblowing Management Team on behalf of your Employer, you will keep a record of internal reports. The register is kept in electronic form and is a record of all reports submitted as part of internal reports.
- 8.7 The register of internal reports includes:
1. Your application number;
 2. the subject matter of the infringement;
 3. personal data of the Whistleblower and the person to whom the report relates, necessary to identify them;
 4. the Whistleblower's contact address;
 5. the date of filing the application;
 6. information on the follow-up actions taken;
 7. the date the case was completed.
- 8.8 Only authorised persons have access to the register. Personal data and other information in the register of internal reports are stored for a period of 3 years after the end of the calendar year in which the follow-up actions were completed or after the end of the proceedings initiated by these actions.

9. Submission to global structures

- 9.1 A whistleblower is also entitled to report a breach of the law in accordance with the global whistleblowing policy in force at the parent company of the Coesia group, i.e. Coesia S.p.A.

10. External application

- 10.1 A whistleblower has the right to report breaches of the law in any case to a central authority (the Ombudsman) or to public authorities in Poland and, where appropriate, also to institutions, bodies, offices or agencies of the European Union (**making the so-called external report**), bypassing the procedure provided for in this Procedure.
- 10.2 The employer encourages the use of internal reporting channels provided for in this Procedure.

11. Protection of whistleblowers

- 11.1 The employer shall provide protection to the Whistleblower in accordance with the provisions of this Procedure and the Act.
- 11.2 Retaliatory actions, or attempts or threats to take such actions, against a Whistleblower are prohibited within the scope indicated by the Act. Retaliatory actions do not include actions or omissions by the Employer that are lawful and justified by objective reasons unrelated to the reported incident. Prohibited retaliatory actions may include, in particular:
1. refusal to establish an employment relationship;
 2. termination of employment, with or without notice;
 3. reduction of salary;
 4. withholding or overlooking promotions;
 5. being overlooked when granting work-related benefits other than salary, or reducing the amount of such benefits;
 6. demotion to a lower position;
 7. coercion, intimidation, or exclusion;

8. harassment or discrimination;
9. unfavorable or unfair treatment.

- 11.3 A Whistleblower subjected to retaliatory actions has the right to compensation as provided for in the Act.
- 11.4 A whistleblower is subject to the protection set out in the Act and Procedure, from the moment of reporting, provided that he or she had reasonable grounds to believe that the information being the subject of the report was true at the time of making the report (the so-called “report in good faith”) and that such information constitutes information about an infringement of the law referred to in Article 2 of the Procedure.
- 11.5 The provisions regarding the prohibition of retaliatory actions also apply to individuals assisting in making the report and to persons associated with the Whistleblower, as well as, accordingly, to legal entities or other organizational units assisting or associated with the Whistleblower, particularly those owned by or employing the Whistleblower.

12. Disabling protection

- 12.1 A person who reports a breach or the possibility of committing it in a manifestly groundless manner or in bad faith, e.g. by deliberately slandering the person to whom the report relates, by certifying untruth (false reporting) or other negative behaviour aimed at putting the person in a disadvantageous position is not protected.
- 12.2 A person who has suffered damage due to a deliberate reporting or public disclosure of false information by a Whistleblower is entitled to compensation or redress for infringement of personal rights from the Whistleblower who made such a report or public disclosure.

13. Familiarizing the Employee with the content of the Procedure

- 13.1 The Employer makes the content of the Procedure available in the manner adopted by the Employer, i.e. on a common drive, in the HR catalogue - policies and procedures and on its website:
<https://www.flexlink.com/en/about-us/business-ethics>.
- 13.2 A person applying for employment with the Employer on the basis of an employment contract or a civil law contract is provided with information about the internal reporting procedure along with the commencement of recruitment or negotiations preceding the conclusion of the contract.
- 13.3 The employer is obliged to familiarize the Employee with the content of the Procedure before allowing him or her to work. A statement of familiarization with the content of the Procedure will be included in the employment contract or in a separate document referred to in paragraph 4 of this paragraph.
- 13.4 The written statement referred to in paragraph 3 of this paragraph, bearing the Employee's signature and date, shall be attached to the employee's personal file.

14. Applicable law and Final Provisions

- 14.1 In matters not regulated by this Procedure, the relevant provisions of Polish law shall apply.
- 14.2 In the event of a change in the generally applicable regulations concerning the matter covered by the Procedure, the new regulations shall replace the previous ones on the date of their entry into force, and the provisions of the Procedure shall be interpreted in accordance with them.
- 14.3 The Procedure comes into effect 7 days after it has been communicated to individuals performing work at the Employer's establishment.

- 14.4 The announcement of the Procedure is preceded by consultations with the company's trade union organization or representatives of individuals performing work for the Employer.

Plewiska, on 01.10.2024