

Whistleblowing Management Procedure

for Coesia S.p.A.
and its Italian subsidiaries

Contents

Part I - GENERAL	3
1. Purpose	4
2. Scope of application	4
3. Principles	5
4. Definitions	6
Part II - WHISTLEBLOWING PROCESS	9
5. Roles and Responsibilities	10
6. Reports	11
7. Reporting person	13
8. Reporting Channels	14
9. Management of the Report	17
10. Prohibition of retaliation	22
Part III - FINAL PROVISIONS	23
11. Protection of Confidentiality	24
12. Continuous improvement process	25
13. Document archiving and traceability	25
14. Training and communication	26
15. Disciplinary measures	27
16. Regulatory framework and Privacy	28
17. Annex A - Privacy Notice	30

Whistleblowing Management Procedure

Recipients: Coesia S.p.A. and its Italian subsidiaries

Approved by: Board of Directors of Coesia S.p.A.

Issued by: CEO of Coesia S.p.A.

Date: July 2026

Version: v. 4.0

Part I

GENERAL

1. Purpose

Coesia S.p.A. and its Italian subsidiaries (hereinafter also “Coesia” or the “Company”), in adherence to its own values, the behavioral principles defined in its Group Code of Ethics, and its commitment to comply with and be compliant with the laws in force, adopts the following procedure for the management of Reports and appropriate channels (the “Procedure”), in line with the Global Whistleblowing Management Procedure, so that all persons operating in the name of and on behalf of Coesia may have available an all-encompassing tool through which to convey Reports of breaches of the Group Code of Ethics, Legislative Decree 231/2001 and Legislative Decree 24/2023.

The purpose of this document is to describe the stages of receipt, assessment, analysis and management of Reports by defining the roles and responsibilities of the process, the subject matter of the Reports, the persons entitled to report, and the management process that the reporting person and the Company will follow.

2. Scope of application

This Procedure applies to Coesia and its Italian subsidiaries and is addressed to all Recipients (the “Recipients”) who, in the context of their professional activities, become aware of a possible breach, including the persons set out in Legislative Decree 24/2023:

- all collaborators of Coesia and the Italian subsidiaries (employees, including those on fixed-term contracts or who perform occasional services, volunteers and interns, self-employed workers, agency workers, collaborators, professionals, consultants);
- persons with powers of representation, administration, or management, or who exercise management and control of company activities (members of corporate bodies);
- persons not yet hired who have become aware of breaches during the selection process;
- customers, contractors, suppliers, partners, agents, and commercial intermediaries who are recipients of the Group Code of Ethics and, more generally, any Group stakeholder.

3. Principles

Recipients of this Procedure who submit a Report (the “Reporting Persons”) and the persons involved in managing the Reporting process must operate in compliance with the general principles established below:

Confidentiality

The identity of the Reporting Person, the reported person, and the other persons involved, as well as the Report (and the related information), must not be disclosed to persons not involved in the management of the Report. It may be communicated, for example, only if strictly necessary for the management of the Report and, in any event, limited to the persons responsible for managing the Report, as described in this Procedure. In this case, the Reporting Person must be informed in advance in writing and provide consent in written form.

Transparency

The activities governed by this Procedure must ensure transparency in the performance of duties and the provision of complete and truthful information.

Impartiality, independence, professionalism, and assurance of the absence of a conflict of interest

Reports must be managed by ensuring the maintenance of the necessary conditions of independence and the necessary objectivity, competence, and professionalism.

The Company ensures that Reports are managed exclusively by persons who are not in a conflict-of-interest position.

Truthfulness and substantiation

Reports must concern information of which the Reporting Person is reasonably certain.

Prohibition of retaliation protecting reporting persons and the other parties involved

The prohibition of retaliation exists if the Reporting Person made the Report on the basis of founded reasons or reasonable suspicions regarding breaches committed or which, on the basis of concrete evidence, could be committed within the organization. This principle also applies pursuant to art. 17(4) of Legislative Decree 24/2023, which regulates and guarantees the prohibition of retaliation against the Reporting Person and protection against any action that may cause unjust harm to the persons involved in the Report.

4. Definitions

Code of Ethics	The Group Code of Ethics published on the intranet and on Coesia's website.
Coesia S.p.A.	Coesia S.p.A. and its Italian subsidiaries.
Group Ethics Committee	Body endowed with independence and autonomy chaired by the Chairman of Coesia. It represents the support structure for the Whistleblowing Manager, as expressly provided by ANAC in the Guidelines adopted with resolution 478 of November 26, 2025, paragraph 3.6 (the "ANAC Guidelines"). The members of the Ethics Committee are Isabella Seràgnoli, Iole Anna Savini, Giorgia Capuzzo, Paolo Fabiani, and Paola Lanzarini.
Reportable Conduct	Conduct, acts, or omissions harmful to the company and consisting of: • Breaches of the Code of Ethics and of Coesia procedures; • Administrative, accounting, civil, or criminal offenses; • Offenses within the scope of acts of the European Union (EU) or national acts; • Breaches of EU rules on competition and State aid; • Breaches of local regulations on social responsibility such as, for example, Legislative Decree 231/2001; • Breaches of applicable national law.
Facilitator	The person who assists the Reporting Person in the Reporting process and who may operate both within and outside the work environment and whose assistance must be kept confidential. By way of example, it may be the Whistleblowing Manager, the direct superior, a colleague, or any other person internal or external to the company. The facilitator enjoys the same protections as the Reporting Person, as governed by paragraph 11. "Protection of confidentiality".

Whistleblowing Manager	These are two members of the Group Ethics Committee who are responsible for the management and coordination of the Reporting process: Paolo Fabiani and Paola Lanzarini.
Navex	The digital platform for Reports identified by Coesia that meets regulatory requirements and ensures the highest standards of security, processing, and protection of sensitive personal data.
Supervisory body	Independent body endowed with powers of control and oversight in relation to the criminal offenses provided for by Legislative Decree 231/2001.
Person Concerned	The subject named in the Report as the person to whom the breach is attributable.
Local Contact Person	Person designated for the management and coordination of the Reporting process in G.D S.p.A. (Paola Lanzarini) and in System Ceramics S.p.A. (Iole Anna Savini).
Retaliation	Any conduct, act, or omission, even if only attempted or threatened, committed as a result of the Report that causes, or may cause, to the Reporting Person, directly or indirectly, unjust harm.
Reporting Person	Anyone who reports a suspected breach as defined under the heading "Reportable Conduct."
Report	Communication made in written or oral form or by request for a meeting, in accordance with the Whistleblowing Management Procedure.
Constructive Reports	New ideas and improvement proposals.

Third parties

- Self-employed and agency workers, collaborators, professionals, consultants;
- Persons not yet hired who became aware of breaches during the selection process;
- Former employees or partners of Coesia who became aware of breaches while they were still in a relationship with the Company.

Part II

WHISTLEBLOWING PROCESS

5. Roles and Responsibilities

Whistleblowing Manager

The Whistleblowing Manager acts as the channel manager pursuant to art. 4(2) of Legislative Decree 24/2023. In addition, in line with the provisions of Legislative Decree 24/2023, one Local Contact Person has also been appointed for G.D S.p.A. and one for System Ceramics S.p.A.

The Whistleblowing Manager is responsible for the following activities:

- a) issuing the reporting person the acknowledgment of receipt of the Report within seven days from the date of receipt;
- b) maintaining communications with the Reporting Person and request any additions;
- c) diligently following up on the Reports received;
- d) providing a reply to the Report within three months from the date of the acknowledgment of receipt or, failing such acknowledgment, within three months from the expiration of the seven-day period from submission of the Report;
- e) making available clear information on the channel, the procedures, and the requirements for making internal Reports, as well as on the channel, the procedures, and the requirements for making external Reports.

In particular, in the performance of its responsibilities, the Whistleblowing Manager is responsible for:

- designing the Reporting process, ensuring its constant updating and that of the Reporting channels, where appropriate;
- diligently following up on the Reports received by coordinating all actors involved in the Report management process;
- entering Reports received in non-written form into the digital platform;
- assessing the admissibility of the Report, with the support of the Ethics Committee and external consultants for Reports pursuant to Legislative Decree 24/2023 and for cases of breach of the Code of Ethics, and of the Supervisory Body for Reports pursuant to Legislative Decree 231/2001, in order to verify that it is not manifestly unfounded or generic in content;
- initiating the internal investigation, in the case of an admissible Report, with the support of the heads of functions within the organization and/or external consultants, identifying the persons responsible for carrying out specific checks, analyses, and assessments regarding whether the reported facts are substantiated or not;
- providing feedback to the Reporting Person within the time limits provided by Legislative Decree 24/2023.

Ethics Committee

The Ethics Committee is a body endowed with independence and autonomy, chaired by the Chairman of Coesia and composed of Isabella Seràgnoli, Iole Anna Savini, Giorgia Capuzzo, Paolo Fabiani, and Paola Lanzarini.

The Ethics Committee receives the Reports and provides support and opinions to the Whistleblowing Manager, especially in the admissibility, assessment, and closure phases of the Report.

6. Reports

In order to increasingly foster a culture of transparency and facilitate the path of continuous improvement undertaken by Coesia, the Reporting channels may be used to report behaviors not aligned with the standards of conduct contained in the Code of Ethics and in the Group Procedures, as well as breaches of Legislative Decree 24/2023 and 231/2001, and also to collect recommendations, suggestions or positive feedback regarding any aspect worthy of attention.

In particular, the breaches pursuant to art. 2 of Legislative Decree 24/2023 are those listed below:

1. administrative, accounting, civil, or criminal offenses that do not fall within points 3., 4., 5. and 6.;
2. unlawful conduct relevant under Legislative Decree 8 June 2001, no. 231, or breaches of the Organization and Management Model adopted by the Company pursuant to the cited legislation and that do not fall within points 3., 4., 5. and 6.;
3. offenses connected to European Union or national acts indicated in the annex to Legislative Decree 24/2023;
4. offenses connected with acts of the European Union or national acts even if not indicated in the annex to Legislative Decree 24/2023, relating to the following sectors: public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radioprotection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and protection of personal data and security of networks and information systems;
5. acts or omissions harming the financial interests of the European Union referred to in Article 325 of the Treaty on the Functioning of the European Union as specified in the relevant secondary law of the European Union;

6. acts or omissions concerning the internal market, referred to in Article 26, paragraph 2, of the Treaty on the Functioning of the European Union, including breaches of European Union rules on competition and State aid, as well as breaches concerning the internal market connected to acts that violate the rules on corporate income tax or mechanisms whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate income tax legislation;
7. acts or behaviors that frustrate the object or purpose of the provisions contained in the acts of the European Union in the areas indicated in points 3., 4. and 5.

Information on breaches must concern behaviors, acts, or omissions of which the Reporting Person has become aware in the work-related context, which harm the public interest or the integrity of the entity.

The following are not, however, the subject of a Report:

- disputes, claims, or requests linked to a personal interest of the Reporting Person, or relating exclusively to their individual employment relationships with hierarchically superior persons;
- information manifestly lacking substantiation;
- information already in the public domain;
- information obtained on the basis of rumors or hearsay that are unreliable (e.g.: "office gossip");
- breaches already governed by other acts of the European Union or national acts (as indicated in the "Part II of the Annex to Decree 24/2023");
- breaches in matters of national security and of procurement relating to defense or national security unless such aspects fall within the relevant secondary law of the European Union.

In order for the Report to be admissible, it is necessary that it, in addition to meeting the objective requirements set forth above, be as detailed as possible. In particular, it is necessary that the following be clear:

- the time and place in which the fact that is the subject of the Report occurred and, where applicable, also the manner through which the Reporting Person became aware of the facts;
- the description of the fact;
- the personal details or other elements, if known and where available, that allow identification of the subject to whom the reported fact is attributable.

7. Reporting Person

Everyone may report. Coesia extends the ability to report to all persons who become aware of a possible Reportable Conduct.

Persons making a Report, in line with this document, are recognized the rights of protection provided by the regulations themselves and indicated in Part III.

Coesia, in line with the principles of its own Code of Ethics, undertakes to ensure confidentiality and protection from any form of retaliation, discrimination, or penalization for persons making a Report of other breaches or a Constructive Report. The Company's ability to make use of the testimony of the Reporting Person remains unaffected, possibly together with other testimony as well, where necessary to protect the Company in the appropriate fora, including judicial ones.

8. Reporting Channels

Coesia, having informed the labor representatives and trade unions, has established, in addition to the Group channel, a dedicated Channel for the companies G.D S.p.A. and System Ceramics S.p.A. for the submission of Reports of breaches pursuant to art. 2 Legislative Decree 24/2023, including those relating to breaches under Legislative Decree 231/2001 and the Group Code of Ethics, which may be submitted according to the following methods.

FOR ALL REPORTS AND BREACHES (OF THE CODE OF ETHICS, PURSUANT TO LEGISLATIVE DECREE 231/2001 AND PURSUANT TO ART. 2 Legislative Decree 24/2023)

- **in written form:**

- through the digital platform for Reports, accessible at the following link from a computer coesia.ethicspoint.com;
- from a mobile phone coesia.navexone.eu, also with the following QR code;
- by sending a signed letter to the following address: **Coesia, Ethics Committee, Via Battindarno 91, 40133 Bologna**. To preserve the utmost confidentiality, it is required that the closed envelope addressed to the Ethics Committee or the Local Contact Person bear the word “confidential” and that such envelope contain two other closed envelopes: (1) one with the Reporting Person’s personal and contact details; (2) the second with the content of the Report.



- **in oral form**

- by **telephone**, (available 24 hours a day, 7 days a week) as indicated on the platform where the toll-free telephone number is available;

(these methods also provide the Reporting Person with the option to choose the anonymous form of Report)

- or by directly contacting the Whistleblowing Manager at the following telephone number **+39 051 6423355**.

- **through physical meeting**

upon written request of the Reporting Person sent by e-mail to codicetico@coesia.com, scheduled to be held within a period of 15 working days, using a private e-mail address, not traceable to the person's company e-mail.

Note for all Reports

Coesia ensures the same safeguards and equal treatment also for all Reports received in anonymous form.

Without prejudice to all the indications contained in this Whistleblowing Management Procedure, **to submit Reports relating to the Code of Ethics or constructive Reports, other internal channels may also be used such as:**

- if one feels comfortable doing so, the Report may initially be discussed with one's **direct supervisor**, who is required to comply with the duty of confidentiality;
- if the report concerns matters relating to **individual or collective disputes**, the relevant human resources officer can be contacted;
- e-mail to **codicetico@coesia.com**.

With reference to the choice to make a Report by sending e-mail, it is understood that the risk mitigation measures adopted by the Company, also in light of the indications implementing the ANAC Guidelines, due to the nature and operation of these technical and information systems, do not guarantee the Reporting Person absolute confidentiality and protection of his or her personal data vis-à-vis the Company. For example, the identity of the Reporting Person could be revealed if the Report is sent using a company e-mail account, or personal e-mail addresses that explicitly show first and last name or other elements suitable to allow the direct identification of the Reporting Person. Identification could, moreover, occur indirectly, through the use of pseudonyms, signatures, or other references which, possibly through association with other available information (for example role, function, or duties publicly attributable to the Reporting Person), make it possible to discover his or her identity. It is understood that, should the Reporting Person choose to use such methods of submission of the Report, the Company will process any personal data acquired exclusively to the extent strictly necessary for the management of the Report, in compliance with the applicable whistleblowing and personal data protection legislation, and in particular Legislative Decree No. 24 of March 10, 2023 and Law No. 179 of November 30, 2017, as well as in accordance with the Privacy Notice available as an Annex to this Procedure, which also illustrates the rights regarding the processing of personal data.

EXTERNAL CHANNEL**ONLY FOR BREACHES PURSUANT TO ART. 2 Legislative Decree 24/2023**

The Reporting Person has the possibility, where certain conditions exist, to also resort to an external channel active at the National Anti-Corruption Authority (ANAC), or any other form provided by law. It is understood that Coesia S.p.A. cannot be held liable if the reporting person has intentionally disclosed his or her identity, including for example through a web platform or social media or any other means, and, in such situations, the protection of confidentiality referred to in Chapter 11 of this document may not be guaranteed.

It is recommended to give priority to the internal reporting channel, limiting the external channel and public disclosure to the specific conditions defined in note 1 of this document.

In using the Reporting channels described above, the Reporting Person may avail himself or herself of the support of a natural person who can assist him or her in the process and who assumes the role of Facilitator.

In particular, the Reporting Person is autonomous in selecting the Facilitator and may identify such person in someone internal or external to the organization. By way of example and not limitation, the Facilitator may also be the Whistleblowing Manager, a direct supervisor, an HRBP, a colleague, a third party, or any other internal or external figure within the organization.¹

¹The external channel at ANAC may be activated under the following conditions:

- the internal channel is not active or is not suitable to ensure the confidentiality of the reporting person;
- the internal channel was used, but the Report was not followed up by the Whistleblowing Manager within the designated time limits or no actions were taken for its management;
- the reporting person has reasonable grounds to believe that use of the internal channel would not be effective or could give rise to a risk of retaliation;
- the Reporting Person has reasonable grounds to believe that the breach may pose an imminent or manifest danger to the public interest (e.g. health and safety or environmental damage).

Public disclosure (through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people) may be used in the following cases:

- the Reporting Person has previously made an internal and external report or has directly made an external report and no response has been given within the time limits provided;
- the Reporting Person has reasonable grounds to believe that the breach may pose an imminent or manifest danger to the public interest;
- the reporting person has reasonable grounds to believe that the external report may entail the risk of retaliation or may not have effective follow-up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed or where there is a well-founded fear that the person who received the Report may be colluding with the perpetrator of the breach or involved in the breach itself.

9. Management of the Report

Internal Reports received through the channels described in the preceding paragraph will be managed in accordance with the procedures set forth below. When the Whistleblowing Manager receives a Report in a form other than written form, the Whistleblowing Manager is required to enter it on the dedicated digital platform. The Company guarantees that Reports are managed exclusively by persons who possess the required impartiality and independence and who are not in a conflict of interest position.

If the names of the Whistleblowing Manager or the Local Contact Person (where applicable), or of members of the Ethics Committee, or of the Supervisory Body in the case of “231” Reports, are cited, or if the aforesaid persons hold the role of Reporting Persons, the Report is forwarded directly to the Ethics Committee, in restricted composition, with the mandatory recusal of the reported or reporting member, so as to ensure effective, independent and autonomous management of the Report.

a. Receipt

This activity is carried out and coordinated by the Whistleblowing Manager, who must inform the Reporting Person that the Report has been received, within 7 days from receipt. The communication does not involve any assessment of the contents that are the subject of the Report, but is merely informational with reference to the receipt of the Report.

This information is accessible to the Reporting Person through an automatic notification e-mail sent by the NAVEX digital platform for Reports, upon any change in the status of the Report itself. The Reporting Person may access the Report on the digital platform through the link received and verify its status, or alternatively through a response to the e-mail or to the letter sent.

If the Report is sent to a person other than the one identified and authorized, the Report must be forwarded by the latter, within 7 days from its receipt, to the competent person, giving simultaneous notice to the Reporting Person.

b. Assessment of the admissibility of the Report received

This activity is carried out by the Whistleblowing Manager with the support of the Ethics Committee and external consultants for Reports pursuant to Legislative Decree 24/2023 or relating to the Code of Ethics and by the Supervisory Body for Reports pursuant to Legislative Decree 231/2001.

This phase aims to:

1. Verify that the Report was made in line with this document;
2. Assess the subject matter of the received Report in order to verify whether

the requirements are met to fall within one of the cases governed by this document (for example, breach pursuant to Legislative Decree 24/2023 or pursuant to Legislative Decree 231/2001, Report of other breaches of the Group Code of Ethics, Constructive Report) or not;

3. Initiate discussions with the reporting person, requesting, if necessary, appropriate supplementary information.

Therefore, the Whistleblowing Manager, with the support of the Ethics Committee or the Supervisory Body depending on the Report's compliance with this document, assesses its admissibility and notifies the Reporting Person thereof.

The Reporting Person may access the Report on the digital platform via the link received and check its status, or will receive communication by e-mail or letter, if these channels of communication were chosen.

Where, instead, the requested supplementary information and clarifications have not been provided, the Manager may archive the Report, in any event providing the Reporting Person with the reasons for the decision.

After ascertaining the admissibility of the Report, the Whistleblowing Manager, with the support of the Ethics Committee, identifies the responsible parties to be involved in the subsequent investigation phase, and sends them the minimum information necessary in order to initiate such phase.

In this regard, it is specified that:

- if the Report concerns a breach pursuant to art. 2 of Legislative Decree 24/2023 or a breach of the Code of Ethics or a Constructive Report, it will be handled by the Whistleblowing Manager and the Ethics Committee, in line with what is provided for in the subsequent paragraphs "c. investigation" and "d. closure" of this document;
- if the Report concerns a breach of Legislative Decree 231/2001, it will be handled by the Supervisory Body.

c. Investigation

This phase is carried out and coordinated by different parties, depending on the type of Report:

- Reports attributable to a case governed by Legislative Decree 24/2023 and the Code of Ethics or Constructive Reports: the person responsible for managing the investigation is the Whistleblowing Manager and the Ethics Committee. The Whistleblowing Manager must initiate the investigation process and ensure that it is carried out within the established time limits;
- Reports attributable to a case governed by Legislative Decree 231/2001: the person responsible for managing the investigation is the Supervisory Body, while the Whistleblowing Manager must initiate the investigation process and ensure that it is carried out within the established time limits.

The party responsible for the investigation phase ensures that inspection activities are carried out and may avail of the operational and technical contribution of the functions and/or external consultants previously identified.

The investigation is intended to carry out targeted inspections that make it possible to identify, analyze, and assess any elements that may substantiate of the reported events.

The investigation phase must be impartial toward the functions concerned, the Reporting Person, and the subject of the Report and must be conducted without prejudice. Furthermore, the subject of the breach must be recognized the right to respond as requested, as well as the opportunity to be assisted.

This phase must be conducted in compliance with the following principles, set forth below by way of example and without limitation:

- the objective and scope of application must be clearly defined and documented;
- the investigation must ensure the security and confidentiality of the parties involved, of the content of the Report, and of the attached documentation;
- personal data must be managed in line with data protection (paragraph “5. Principles”);
- the communication must be clear and free of ambiguity;
- the Reporting Person must be periodically informed of the progress made. Moreover, the Human Resources function is involved in the investigation phase to ensure the implementation of protection measures for the Reporting Person and the reported person, and to assess the impacts from an employment law perspective.

d. Closure

This phase is carried out and coordinated by the Whistleblowing Manager, having consulted the Ethics Committee or the Supervisory Body, depending on the subject matter of the Report, and the heads of internal functions within the organization and/or external consultants involved in the preceding phases.

The closing phase indicates the end of the Reporting process.

A case must be closed if no further actions are deemed necessary and no further checks must be carried out.

During this phase, the following steps must be taken into consideration:

- conclusion of the Report and communication of the result to the reporting person;
- actions in response to any indications (for example, disciplinary actions);
- communication to the personnel responsible for supporting and protecting the Reporting Person and to the other interested parties;
- identification of any protection measures in place;
- collection of suggestions from the reporting person and the other interested parties;
- archiving of the documents produced during the preceding phases.

If, during the assessment phase, the breach has been confirmed, the head of the function to which the subject matter of the Report refers (provided it is deemed to be well-founded), may be involved in defining the action plan relating to the areas and processes affected by the Report.

Moreover, the Whistleblowing Manager, in agreement with the Ethics Committee, and with the support of the functions and/or consultants involved at the investigation stage, shall proceed to:

- formalize any corrective measures for the resolution of the breach;
- involve Internal Audit in verifying the proper application of any corrective measures;
- receive regular updates on the effectiveness of the monitoring measures;
- define disciplinary measures, if applicable;
- involve the competent authorities, if necessary. In such case, where the identity of the Reporting Person is requested by the judicial or accounting authority, the Whistleblowing Manager shall provide such information, upon prior notice to the Reporting Person.

At the end of the closing phase, the Whistleblowing Manager, in agreement with the Ethics Committee or with the Supervisory Body, depending on the nature of the Report, and with the support of the functions and/or consultants involved, provides feedback on the Report. Such information is accessible to the

Reporting Person through an automated notification e-mail sent by the digital platform for Reports upon each change in the status of the Report itself. The Reporting Person may access the Report on the digital platform through the link received and verify its status, or alternatively through a response to the e-mail or to the letter sent.

The feedback provided in such communication must account for the outcome of the Report and, in particular, by way of example, such communication may be:

- **archived** for lack of substantiation, absence of sufficient evidence, or other reasons;
- **closed** with measures taken in order to resolve the issue raised;
- **referred** to a competent authority for further investigations.

The Whistleblowing Manager must provide an initial response, even if only provisional, to the reporting person within three months from the date of the acknowledgment of receipt or, failing such acknowledgment, within three months from the expiration of the seven-day period following submission of the Report. The aforesaid deadline is not intended to be strictly binding.

e. information flows with the Supervisory Body

The Whistleblowing Manager, as provided for by the Organization and Management Model, shall be required to periodically provide an appropriate information flow to the Supervisory Body, with reference to reports concerning the offenses referred to in Legislative Decree 231/2001.

10. Prohibition of retaliation

With respect to the Reporting Person, no **form of retaliation** or **discrimination** directly or indirectly connected to the Report will be tolerated. Retaliation includes, for example:

- dismissal, suspension, or equivalent measures;
- demotion or non-promotion;
- change in functions, the change of the place of work, the reduction of salary, the modification of working hours;
- suspension of training or any restriction on access thereto;
- negative merit notes or negative references;
- adoption of disciplinary measures or any other sanction, including monetary sanctions;
- coercion, intimidation, harassment, or ostracism;
- discrimination or, in any event, unfavorable treatment;
- non-conversion of a fixed-term employment contract into an open-ended employment contract, where the worker had a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to a person's reputation, in particular on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- inclusion in improper lists on the basis of a formal or informal sectoral or industry agreement, which may result in the person's inability to find employment in the sector or industry in the future;
- the early termination or cancellation of the supply contract for goods or services;
- the cancellation of a license or a permit.

Part III

Final

Provisions

11. Protection of Confidentiality

The name of the Reporting Person and any other information from which his or her identity may be inferred, directly or indirectly, may not be disclosed to persons other than those competent to receive or act upon the Reports and expressly authorized to process such data, without the express consent of the Reporting Person.

In particular, with regard to the disclosure of the identity of the reporting person, Legislative Decree 24/2023 (art.16) provides the following protections:

- Within the scope of criminal proceedings, the identity of the reporting person is covered by secrecy, in the manner and within the limits provided for by article 329 of the Code of Criminal Procedure (paragraph 3);
- Within the scope of disciplinary proceedings, the identity of the reporting person may not be disclosed where the contestation of the disciplinary charge is based on findings that are distinct and additional to the Report, even if they result from it. If the contestation is based, in whole or in part, on the Report and knowledge of the identity of the reporting person is indispensable for the defense of the accused person, the Report may be used for the purposes of the disciplinary proceeding only in the presence of the express consent of the reporting person to the disclosure of his or her identity (paragraph 5);
- The reporting person shall be given notice by written communication of the reasons for the disclosure of the confidential data, in the case referred to in paragraph 5, second sentence, as well as in the internal and external reporting procedures referred to in this chapter when the disclosure of the identity of the reporting person and of the information referred to in paragraph 2 is indispensable also for the purposes of defending the person concerned (paragraph 6).

Confidentiality is also guaranteed:

- in the case of Reports, internal or external, made orally through telephone lines or at the request of the reporting person, through a physical meeting with the person handling the Report;
- when the Report is made through means other than those established in accordance with the decree or is received by personnel other than those authorized and competent to handle Reports;
- to the reported person and to persons different from the reported person but mentioned in the Report or involved in the Reporting process.

12. Continuous improvement process

In addition to what is indicated above in this Procedure, it shall be the Company's responsibility to define any recommendations regarding the adoption of the necessary corrective actions in the areas and company processes affected by the Reports and to monitor the status of implementation of the aforesaid corrective actions, in order to activate a virtuous path of continuous improvement of the internal control system.

13. Document archiving and traceability

Reports must be traceable in compliance with privacy requirements.

In the event of a Report made orally or through a physical meeting concerning the breaches referred to in Legislative Decree 231/2001 and 24/2023, the Report must be traced by means of:

- recording of the conversation or meeting, subject to the authorization of the reporting person;
- drafting of minutes of the meeting, which must be signed by the Reporting Person for approval (with prior opportunity for review and correction);
- documentation of the Report on the digital platform for Reports by the Whistleblowing Manager, following the conclusion of the conversation or meeting.

All documents relating to the Report must be retained for as long as necessary to manage it. The obligation to retain the documentation relating to the Report lapses after 5 years from the date on which the outcome of the Reporting process was communicated to the reporting person. Upon expiration, the documentation shall be deleted.

14. Training and communication

Coesia, in accordance with its values and the behavioral principles as set forth in the Group Code of Ethics, is committed to implementing appropriate measures to raise awareness among employees and third parties regarding the Reporting System, including its procedures, the process to be followed, and the requirements to be met.

Training provided to personnel and collaborators is organized upon the hiring of personnel and updated regularly, in the event of significant regulatory changes, in line with the roles and involvement in the Reporting process.

Such internal training must address the following aspects:

- the worker's contribution to the effectiveness of the Whistleblowing Management System;
- how to recognize breaches;
- how and to whom it is possible to report a suspected breach;
- how and to whom it is possible to ask questions about the Whistleblowing Management System;
- how it is possible to help prevent, avoid, and protect oneself from harmful conduct;
- the protections available in the event of use of the Whistleblowing Management System;
- the impact of the failure to report a breach and its potential consequences;
- the consequences of actions resulting from non-compliance with the Reporting Procedure, such as, for example, knowingly submitting false Reports, and how harmful conduct may justify disciplinary action.

This Procedure does not replace what is already provided by law, which shall remain valid and binding for all recipients; in particular, the Whistleblowing Management System does not replace local legal obligations to report to the competent authorities, where applicable, nor does it constitute a waiver or assumption of any specific liability for the organization's top management.

Furthermore, in order to make Third Parties aware of this Procedure, a specific procedure to be accepted at the time of signing is inserted within contractual documentation.

Information regarding the channels, procedures, and prerequisites for making internal, external, or public disclosure Reports is made easily visible in the workplace, on the intranet, on the website of Coesia and its controlled companies.

15. Disciplinary measures

Coesia and all companies to which this Procedure applies, in accordance with the provisions of Legislative Decree 24/2023, may define disciplinary measures in the event that the criminal liability of the Reporting Person for the offenses of defamation or slander, or in any event for the same offenses committed with the complaint to the judicial or accounting authority, or his or her civil liability, for the same title, in cases of willful misconduct or gross negligence, has been ascertained, even by a judgment of first instance or similar judicial measure. Furthermore, such persons shall not be recognized the protection rights provided for by the regulations themselves. Similarly, Coesia reserves the right to take disciplinary measures or any other appropriate action against anyone who retaliates, or threatens to retaliate, or hinders the Report or contravenes the provisions of this Procedure, without prejudice to the right of the parties involved to take legal action where criminal or civil liability has been found in connection with the falsity of what has been stated or reported.

16. Regulatory framework and Privacy

Main regulatory framework and other relevant references that constitute the basis of this Procedure and its processes:

- EU Directive no. 1937/2019 on the protection of persons who report breaches of Union law and related local transpositions;
- Legislative Decree no. 24/2023 "Implementation of 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 and laying down provisions regarding the protection of persons who report breaches of national legal provisions";
- other local regulations relating to the Organization, Management and Control Model (pursuant to Legislative Decree 231/2001 "Administrative liability of entities");
- ISO 37002 "Whistleblowing Management Systems";
- EU Regulation No. 679/2016 "General Data Protection Regulation – GDPR" and related local transpositions.

Personal data must be managed in compliance with EU Regulation No. 679/2016 and the related local transpositions.

All personal data not useful for the management of the Report must not be collected. Furthermore, in the event of accidental collection, such data must be deleted immediately.

The processing of personal data shall be handled in accordance with Regulation (EU) 2016/679 (GDPR), as well as any other applicable law and/or regulation.

Both the Reporting Person's personal data – if the Report is not anonymous – and the personal data of the person concerned and/or any third parties, as well as any further information collected within the investigation necessary and appropriate to ascertain and verify whether or not the Report is well-founded, shall be processed.

Coesia S.p.A. – and, in particular, each Company of the Coesia Group – shall in any event act as an autonomous data controller.

If there is a risk that the exercise of the rights recognized pursuant to Chapter III of the GDPR may result in actual and concrete prejudice to the confidentiality of the Reporting Person's identity, and that the ability to effectively verify the substantiation of the Report or to gather the necessary evidence may be compromised, the right is reserved to limit or delay the exercise of such rights, in accordance with the applicable statutory provisions. In no case may the

person concerned or third parties exercise the right of access in order to obtain information on the identity of the Reporting Person.

For Reporting Persons and reported persons, a notice on the processing of personal data is available, attached to this Procedure.

Coesia S.p.A. reserves the right to assess, on a case-by-case basis, the specific circumstances and conditions that make it appropriate to specifically inform the person concerned of the conclusion of the verification procedure initiated, in order to prevent abuses and, in any event, to ensure the protection of the rights of the data subject.

17. Annex A - Privacy Notice

Privacy legislation provides that a person making a Report with personal data must be informed of the methods of collection and storage of the information submitted.

The Data Controller

The data controller is, from time to time, the Coesia group company to which the Reporting Person and/or the reported person belongs (hereinafter, “**Coesia**”, “**we**”, “**our**” or the “**Company**”). The companies of Coesia share a single channel for reporting Reportable Conduct.

Use of Navex

Use of Navex is entirely optional.

Navex is a confidential online reporting service that allows the Reporting Person to report to their organization certain matters regarding alleged breaches of the law or company policies and to submit questions regarding clarifications and any doubts.

All information submitted will be treated in the strictest confidence, as provided for in the Whistleblowing Management Procedure.

What personal data and information are collected and used?

The following personal data may be processed:

- common identifying and contact data of the Reporting Person and the Facilitator and employment relationship with the organization (unless the report is anonymous);
- identifying data of the persons involved in the Report, information and data relating to the reported breaches;
- any other information relating to the Reporting Person or the reported person, to the persons involved in the Report, which the Reporting Person decides to share in order to better represent the facts described in the Report.

It is not possible to determine in advance the information that is the subject of the Report, which may therefore also include special data or data relating to criminal convictions and offenses.

Coesia urges the Reporting Person not to include in the Report strictly personal data relating to the Reporting Person, the reported person or third parties, that are not connected to the Report.

The provision of the identifying data of the Reporting Person is optional. With regard to the reported person or third parties, the source of the data will be the Report received as well as any other information collected during the course of the investigation process into the Report.

How will personal data and information be processed after the report and who will have access to such data and information?

The Company uses platforms and technological tools made available by third-party providers who are appointed data processors. In some cases, with reference to the provision of administrative or technical services, or in order to allow compliance with its internal procedures, the data may also be communicated among the Companies within the Coesia Group.

In particular, the personal data and information provided will be stored in a database on servers hosted and managed by NAVEX, Inc. in the USA or in the UK. NAVEX is compliant with the EU-U.S. Data Protection Framework ("EU-U.S. DPF"), the UK Extension to the EU-U.S. Framework ("UK Extension"), as established by the United States Department of Commerce.

The personal data could be transferred to the USA or to another country that may not guarantee the same personal data protection measures applied by the European Union.

Where adequacy decisions do not exist or in cases where the transfer becomes necessary (for example, in the case of IT service providers or management platforms located in third countries) the Data Controller shall adopt every appropriate and necessary contractual measure to ensure an adequate level of data protection, including, among others, the Standard Contractual Clauses for the transfer of data outside the EU approved by the European Commission. A copy of the safeguards adopted may be requested by writing to the address dpo@coesia.com.

The personal data will be processed by the Whistleblowing Manager, by the Local Contact Person as well as by the Ethics Committee. Such persons are required to ensure the confidentiality of the identity of the Reporting Person and of the information of which they have become aware.

Where necessary, for requirements connected with the investigative activities, some information related to the report may be processed by:

- consulting, auditing, or security companies or parties carrying out services instrumental to the purposes indicated above, limited to the information necessary for the functions assigned to them, subject to appointment as data processor;
- third parties whose involvement is necessary for the proper analysis of

the Report, such as the legal counsel used by the Company to conduct the relevant interviews, who may act in the capacity of data controllers;

- the Judicial Authority and/or the competent Authorities, who act in the capacity of data controllers.

For what purposes will personal data be processed?

Personal data will be collected and processed for purposes connected with:

- a) the management of Reports as set out in the Whistleblowing Management Procedure for Coesia S.p.A. and its Italian subsidiaries;
- b) enabling the Company to provide feedback to the Reporting Person regarding the Report and maintaining the necessary exchanges with them;
- c) ensuring that the Company complies with the standards of conduct established by the Code of Ethics;
- d) initiating internal investigations and checks regarding compliance with the regulations applicable to the Company;
- e) taking the necessary internal measures in the event of breaches.

On what legal basis will personal data be processed?

Processing of the data arises from the need to comply with a legal obligation (art. 6, paragraph 1, lett. c of the GDPR) and specifically with EU Directive 2019/1937, concerning the protection of persons who report breaches of Union law, implemented in Italy by Legislative Decree 24/2023. In Italy, processing may also take place to enable the Company to comply with Legislative Decree 231/2001 concerning the liability of entities for administrative offenses dependent on a criminal offense.

If special categories of data necessary for the management of the report are processed, processing will be justified pursuant to art. 9, paragraph 2, lett. b) and/or f) of the GDPR, when:

- a) necessary for carrying out the obligations and exercising the specific rights of Coesia or of the data subject in the field of labor law and social security and social protection, insofar as it is authorized by Union law or the law of the Member States or by a collective agreement pursuant to the law of the Member States,
- b) necessary for the establishment, exercise, or defense of a right in judicial proceedings or whenever judicial authorities exercise their judicial functions.

Moreover, the data, except for special categories of data, may be processed, also with reference to the management of reports relating to the Code of Ethics:

- a. to verify and improve compliance with its internal policies on the basis of Coesia's legitimate interest in verifying the correctness of its activities with respect to the applicable regulations that may harm the public interest or the integrity of the Company (art. 6, paragraph 2(f) of the GDPR);
- b. to take, if necessary, appropriate judicial, disciplinary, and administrative actions on the basis of the Company's legitimate interest in exercising and defending its rights (art. 6, paragraph 2, lett. f of the GDPR).

In such cases, any processing of special categories of data that may be communicated by the Reporting Person for such purpose shall take place to the extent strictly necessary to establish and defend a right in judicial proceedings (art. 9 paragraph 2 lett. f GDPR).

For how long will my personal data be retained?

Reports and the related documentation are retained for the time necessary for the processing of the Report and, in any event, for no more than five years from the date of communication of the final outcome of the Reporting Procedure, in compliance with the Reporting Person's confidentiality obligations.

Personal data that are manifestly not useful for assessing the Report shall be immediately deleted.

What rights are provided with respect to the processing of personal data?

Under certain conditions, the rights provided for by arts. 15, 16, 17, 18, 19, 20 and 21 of the GDPR may be exercised and, in particular:

- a) the right to request confirmation as to whether personal data are being processed, to obtain a copy thereof, as well as to obtain information regarding the related processing;
- b) the right to request rectification, updating, or supplementation;
- c) the right to request erasure if
 - i. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - ii. the data were unlawfully processed;
 - iii. you have withdrawn the consent on the basis of which the Company had the right to process the data and there is no other legal basis permitting the processing activity;
 - iv. you have objected to the processing activity and there is no overriding legitimate grounds;
 - v. the personal data must be erased in order to comply with a legal obligation.

The Company shall, however, have the right to disregard the exercise of the

aforementioned erasure rights if the right to freedom of expression and information prevails or for the exercise of a legal obligation or to defend a right in court.

- d) the right to object, in whole or in part, to any processing carried out on the basis of the legitimate interest for reasons related to your particular situation.

The Company shall, however, have the right to disregard the exercise of the right to object in the presence of demonstrated compelling legitimate grounds that prevail over the data subject's interests, rights, and freedoms or for the establishment, exercise, or defense of a right in judicial proceedings;

- e) the right to withdraw consent to processing, where given, freely and at any time;
- f) the right to data portability, namely the right to receive personal data in a structured, commonly used, and machine-readable format, and the ability to transmit them to another data controller freely and without hindrance, limited to processing based on consent or contractual necessity;
- g) the right to request restriction of processing when one of the following circumstances occurs:
 - i. for the period necessary for the Company to verify the accuracy of such personal data of the data subject who has contested their accuracy;
 - ii. in case of unlawful processing of personal data and objection to erasure;
 - iii. if the personal data are not necessary for the purposes of processing but, in any event, you need them to be processed for the establishment, exercise, or defense of a right in judicial proceedings;
 - iv. for the period necessary to verify the possible prevalence of the Company's legitimate grounds over a request to object to processing;
- h) the right to lodge a complaint with the DPA for the protection of personal data, if you believe that the processing has been carried out in breach of the applicable legislation.

The exercise of such rights is subject to certain exceptions in order to:

- a) protect the interest in the confidentiality of the Reporting Person's identity, or
- b) the conduct of defensive investigations or the exercise of a right in judicial proceedings.

In the event of the exercise of any of the aforementioned rights, Coesia and the DPO will verify the legitimacy of the exercise and will respond, as a rule, within one month.

To exercise the rights vis-à-vis the Company, it is possible to contact the following e-mail address: **codicetico@coesia.com**.

The Company has appointed a *Data Protection Officer* who may be contacted at **dpo@coesia.com**.