

# **Whistleblowing Data Protection Privacy Policy**

Information pursuant to Article 13  
of Regulation (EU) 2016/679

# Contents

<b>General Data Protection Regulation, hereinafter “GDPR” “Information”</b>	<b>3</b>
1. Categories of personal data processed	4
2. Purposes of the data processing	5
3. Retention of personal data	6
4. Data processing methods	6
5. Data Controller, authorized categories and Data Protection Officer	7
6. Categories of third parties to whom data can be disclosed	7
7. Data Subject’s rights	8

# **General Data Protection Regulation, hereinafter “GDPR” “Information”**

Coesia S.p.A. (hereinafter “Coesia” or “Data Controller”) invites you to acknowledge the information on the processing of personal data collected for the purpose of receiving, analyzing, investigating and managing reports, and any consequent actions, in accordance with the Global Whistleblowing Policy (hereinafter, “Procedure”), adopted by Coesia and the Coesia Group Companies, in order to strengthen awareness, sensitivity and implementation of the principles and rules of conduct provided for by the Group’s Code of Ethics, and to adapt the organization of all Coesia Group Companies to the supranational, Community, national and local regulations applicable in any capacity, in matters of corporate compliance, including, but not limited to, anti-corruption, anti-money laundering, and whistleblowing.

Please refer to the Procedure for correspondence with the definitions set out in capital letters and to the GDPR – which constitutes a benchmark for the processing of personal data worldwide – for the meaning of the terms relating to personal data processing.

## 1. Categories of personal data processed

The Personal Data collected and processed are those contained in the report, made verbally or in writing through the digital reporting platform (Navex) or by e-mail or letter, as well as those acquired during subsequent investigative activities.

Common personal data referred to in Article 4, point 1, of the GDPR subject to processing may include:

- a. Whistleblower data, in the case of non-anonymous Reports, such as personal data (e.g. name, surname, date and place of birth), contact data (e.g. landline and/or mobile phone number, email address), data relating to the role they hold within Coesia or the Coesia Group Companies or, in the case of an external organization, the entity where they carry out their activity;
- b. data suitable for identifying the subject, framed within Coesia or a Group Company, to whom the facts covered by the report are attributed;
- c. data suitable for identifying any third parties that may confirm the report’s validity;
- d. information contained in the report and relating to the Whistleblower, the reported person, or and third parties involved or mentioned in the Report or the Facilitators, as defined by the Procedure (hereinafter, all referred to as “Data Subjects”).

The Data Controller may also process special categories of data pursuant to Article 9 of the GDPR, if included in the Report.

In compliance with applicable laws, the Data Controller may process personal data, including data relating to third parties, already available to the Data Controller..

## 2. Purposes of the data processing

The aforementioned personal data are processed by the Data Controller for the following purposes:

- a. **Data processing purposes:** management of the Report, carried out according to the provisions set out in the Procedure and in applicable local regulations; performance of related investigative and instrumental activities aimed at verifying the validity of the reports; adoption of corrective measures;
- b. **Compliance purposes:** fulfillment of obligations provided for by the applicable law on the matter;
- c. **Defensive purposes:** defense or ascertainment of the Data Controller's rights in civil, administrative or criminal disputes, as well as for any needs of internal control, monitoring of corporate risks.

The legal basis for the processing is;

- for the purposes referred to in letter a) (Data processing purposes), the fulfillment of a legal obligation to which the Data Controller is subject (Article 6, paragraph 1, letter c) of the GDPR); in addition, for recorded reports collected by telephone or through voice messaging systems or in any case in oral form, the Whistleblower's consent (Article 6, paragraph 1, letter a) of the GDPR);
- for the purposes referred to in letter b) (Compliance purposes), the fulfillment of a legal obligation to which the Data Controller is subject (Article 6, paragraph 1, letter c) of the GDPR and – limited to special data categories – Article 9, paragraph 2, letter g) of the GDPR);
- for the purposes referred to in letter c) (Defensive purposes), from the legitimate interest of the Data Controller (Article 6, paragraph 1, letter f) of the GDPR and – limited to special data categories – Article 9, paragraph 2, letter f) of the GDPR).

It should be noted that access to data is essential for fulfillment of the aforementioned purposes; complete or partial lack of or incorrect access could result in the inability to manage the Report

### 3. Retention of personal data

In compliance with the principles of minimization and limitation of storage, formulated at supranational level (e.g., for EU Member Countries, by Article 5, paragraph 1, letters c) and e) of the GDPR), and nationally, Coesia stores any personal data for the time necessary to process the Report, and in any case, according to the term provided for by Italian law (Article 14 of Legislative Decree no. 24/2023), for no more than 5 years from the date of communication of the final result of the Report to the Whistleblower. However, if national laws require it, the Data Controller reserves the right to retain the personal data collected for a shorter period of time, as well as to retain them for as long as necessary to fulfill Compliance Purposes or Defensive Purposes, it being understood that, in the event that a judgment is established, the terms indicated above may be extended until the conclusion of the judgment itself and the consequent limitation periods. After the times indicated above, the Data contained in the Reports and any accompanying documentation will be deleted and/or anonymised.

Personal data not useful for the processing of a specific Report shall not be collected or, if collected incidentally, shall be promptly deleted.

### 4. Data processing methods

Personal data will also be processed with automated tools for the time strictly necessary to achieve the purposes for which they were collected and, in any case, in order to guarantee their security and confidentiality. At every stage, the Whistleblower Report management system guarantees

- confidentiality over the identity of the Whistleblower, the persons involved and/or in any case mentioned in the Report, the content of the Report and the related documentation, as well as that of any external parties involved (subject to the necessary and proportionate needs in relation to investigations by the competent authorities or judicial proceedings),
- data protection with respect to their alteration, destruction, loss, theft or improper or unlawful use.

## 5. Data Controller, authorized categories and Data Protection Officer

The Data Controller for personal data is each company belonging to the Coesia Group to which the reported conduct refers, it being understood that all Group companies transpose Coesia's decisions regarding the structure and members of the Report Management Team, the identity of the data processors and any other aspect defined in the Procedure.

As indicated in the Procedure, the Reports are managed by the Report Management Team, and data can be disclosed to the data processors identified therein.

Coesia has appointed a Data Protection Officer, who can be contacted at the following email address: **dpo@coesia.it**

## 6. Categories of third parties to whom data can be disclosed

Given the global scope of the Procedure, the processing of personal data of Data Subjects can be carried out by all Coesia Group companies, wherever they are located.

In addition, within the limits of the provisions of locally applicable law and in accordance with the Procedure, some processing may be carried out by additional third parties, to whom Coesia, in agreement with the individual Coesia Group Companies involved, entrusts certain activities (or part of them) for the purposes referred to in point 2); these subjects – in addition to the provider of the digital reporting platform (Navex) – based on the circumstances, will operate as independent Data Controllers or will be designated Data Processors and are essentially included in the following categories: a. Consultants (Law Firms, etc.), b. Companies in charge of personnel administration and management, c. Audit/Auditing Firm, d. Investigative agencies, and. Institutions and/or Public Authorities, Judicial Authorities.

With exclusive reference to EU Member Countries: if the personal data collected are transferred to a non-EU Country or international organizations, the data transfer is carried out by virtue of the existence of a decision of the European Commission on the adequacy of the level of data protection of the non-EU

Country, or on the basis of appropriate and suitable guarantees, provided for by Articles 46 or 47 of the GDPR, or the additional conditions of legitimacy of the transfer provided for by Article 49 of the GDPR.

## **7. Data Subject's rights**

The Data Subject has the right to request access to data concerning them at any time, and to exercise, where applicable, the right of access to personal data, the right to update them, the right to obtain their cancellation (or so-called 'right to be forgotten'), the right to limit their processing, the right to portability of personal data, and the right to object to their processing, as well as any additional rights recognized by local regulations, by sending a notification using the same channel chosen for reporting (Navex platform, email or letter).

The aforementioned rights cannot be exercised by the person mentioned in the Report, for the time and within the limits in which this constitutes a necessary and proportionate measure to avoid an effective and concrete prejudice to the protection of confidentiality of the Whistleblower's identity, as provided, by way of example, by Article 23, paragraph 1, letter i) of the GDPR and recital 85 of EU Directive 2019/1937.