INFORMATION ON THE PROCESSING OF PERSONAL DATA PURSUANT TO ARTICLES 13 AND 14 OF EU REGULATION 2016/679 (GDPR)

Pursuant to EU Regulation 679/2016 ("GDPR"), the CESVI Foundation provides below information regarding the processing of your personal data (as a whistleblower, reported person, person affected by the report, facilitator, etc.), for the purpose of managing reports made through the internal reporting channel provided for by Legislative Decree no. 24 of 10 March 2023 entitled "*Implementing 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 on the protection of persons who report breaches of domestic regulatory provisions*" (hereinafter, for the sake of brevity, the "Decree").

Data Controller

The Data Controller of personal data is the CESVI Foundation with registered office at via Broseta 68/a, 24128, Bergamo.

The data are processed by the Supervisory Body of CESVI and by any CESVI employees authorised to process them. Any communications with the Data Controller, including requests to exercise the rights granted to the Data Subject, must be made using the internal reporting channels activated by the CESVI Foundation, which guarantee the protection of the confidentiality of the Data Subject.

Personal Data Protection Officer

The Data Controller hereby notifies that it has appointed a **Personal Data Protection Officer (DPO)** in accordance with the provision set forth in Article 37, para. 1, letter a) of the GDPR, which can be contacted at the following address:

E-mail: dpo@cesvi.org

The Tasks and functions of the DPO thus designated are set forth in Article 39, para. 1 of the GDPR. The Data Processor is bound by a duty of secrecy or confidentiality regarding the fulfilment of its tasks, in accordance with Union or Member State law; the reports received by the Data Processor are therefore considered confidential.

Types of data processed

The Data Controller will process your personal data (as defined by Article 4 (1) of the GDPR) as provided by you, or otherwise collected, in the context of the procedures for managing the reports received.

The whistleblower is, according to the Decree, the natural person who reports information on violations of which they become aware within their work context (Article 2, para. 1, letter g), of the Decree), or in the context of work or professional activities, present or

past and where there is a risk of retaliation in the event of public reporting or disclosure or the filing of a complaint with the judicial or accounting authority (Article 2, paragraph 1, letter i) of the Decree). The protection provided by the Decree applies not only if the report is made during the employment relationship or other type of legal relationship, but also before or after the establishment of the legal relationship and, in particular, if the information was acquired during the recruitment process or at other pre-contractual stages, or during the probationary period, as well as after the dissolution of the legal relationship if the information on violations was acquired during the latter (Article 3, paragraph 4, of the Decree).

Only information on violations committed or not yet committed but which the whistleblower reasonably believes may be committed on the basis of concrete evidence is reportable. The following are excluded from reportable conduct: the subject of labour disputes, even in the pre-litigation phase, as well as discrimination between colleagues, interpersonal conflicts between the whistleblower and another worker or line managers, reports relating to data processing carried out in the context of the individual employment relationship in the absence of any injury to the public interest or the integrity of the public administration.

The acquisition and management of reports gives rise to the processing of personal data, also included in specific data categories and possibly relating to criminal convictions and crimes which may be included in the report and in deeds and documents attached to it, referring to data subjects (identified or identifiable natural persons) and, in particular, the whistleblowers or persons indicated as potential perpetrators of illegal conduct or those who in various capacities are involved in the events reported (Article 4, para. 1, nos. 1) and 2) of the GDPR).

In the event that access to the internal reporting channels is made from the Data Controller's internal data network, the non-traceability of the whistleblower is guaranteed at the time the connection to these channels is established.

Purposes and conditions of lawfulness of the processing

The processing of personal data carried out by the Data Controller, as part of the management of internal reporting channels is necessary to fulfil the **legal obligations** and perform **tasks of public interest** provided for by the Industry regulations, the observance of which is a condition for lawfulness of the processing (Articles 6, para. 1, letters c) and e) and paras. 2 and 3, 9, para. 2, letters b) and g), 10 and 88 of the GDPR, as well as 2-ter and 2-sexies of the Code).

In certain circumstances, summarized below, the acquisition of the **consent** of the Data Subject is required.

The identity of the whistleblower and any other information from which their identity may be inferred, directly or indirectly, may not be disclosed, without the express consent of the whistleblower, to persons other than those competent to receive or follow up reports and who are expressly authorised to process such data (Article 12, paragraph 2, of the Decree).

In the context of disciplinary proceedings, if the charge is based, in whole or in part, on the report and knowledge of the identity of the whistleblower is essential for the defence of the accused, the report may be usable for the purposes of disciplinary proceedings only given the whistleblower’s express consent to the disclosure of their identity (Article 12, paragraph 5, of the Decree).

Optional or compulsory provision

The provision of data that allow identification of the whistleblower is **optional.** However, failure to provide them could compromise the satisfactory outcome of the preliminary investigation. Even in the case of reports without personal data of the whistleblower, the latter may be, in certain circumstances, identifiable by contextual elements. Therefore, in such cases, the reports will not be considered anonymous in a technical sense and will benefit from the guarantees provided by law.

Failure to provide the whistleblower's contact details, in the event of non-use of the platform set up by the Data Controller, will not allow the exchange of communications and the possible incorporation of information and documents, for the purposes of the investigation.

The whistleblower is at all times responsible for the accuracy and updating of the data provided, even if they relate to the persons indicated as possibly responsible for the illegal conduct or those for various reasons are involved in the events reported.

Personal data that are **manifestly not useful** for the processing of a specific report are not collected or, if accidentally collected, are deleted immediately.

Processing

The Data Controller, as part of the necessary identification of the technical and organizational measures capable of guaranteeing a level of security appropriate to the specific risks for Data Subjects in the delicate context in question, has prepared its own report management model in accordance with the principles of “data protection by design” and “protection by default” (Articles 5, paras. 1, and paras. 2, 24, 25 and 32 of the GDPR) also taking into account the observations submitted in this regard by the Data Protection Officer (DPO).

Considering that the processing of personal data through the report acquisition management systems presents specific risks to the rights and freedoms of the data subjects – also due to the particular sensitivity of the information potentially processed, the vulnerability of the data subjects in the work context, as well as the specific requirements for non-disclosure of the identity of the whistleblower provided for by the Industry legislation – and as expressly provided for by the Decree (Article 13, para. 6), the Data Controller has prepared a specific model for receiving and managing reports, based on a data protection impact assessment.

The Data Controller has set up an email channel for internal reports that guarantees non-disclosure of the identity of the whistleblower, the person involved and the person

named in the report, as well as the content of the report and the related documentation (without prejudice to the possibility of submitting a report even by telephone or during in-person meetings with authorized staff). Whistleblowers are invited to use only the channels specifically established to submit reports, given that these channels offer greater guarantees in terms of security and confidentiality, although even in the event that a report is sent in error through alternative channels, the confidentiality of the identity of the whistleblower and the protection of the data of all data subjects will still be ensured.

Personal data are processed by the Supervisory Body and by staff who may be vested with delegated powers and adequately trained in this regard. In any case, the data will be processed by staff expressly authorized pursuant to Articles 29 and 32, para. 4, of the GDPR and Article 2-quaterdecies of Legislative Decree no. 196 of 30 June 2003 (Privacy Code).

The main processing operations that will be carried out with reference to your personal data are the collection, registration, organization, structuring, storage, consultation, use and communication thereof.

The processing of your personal data will be carried out both manually and using IT and telematic systems, with organization and processing logic strictly related to the actual purposes and in any event, in a manner that guarantees the security, integrity and confidentiality of the data in compliance with the organizational, physical and logical measures provided for by the provisions in force. **The activation of an automated decision-making process is excluded.**

The reports will not be used beyond what is necessary for their adequate follow-up (Article 12, paragraph 1, of the Decree).

Disclosure and dissemination of personal data

Your personal data may be disclosed to:

1. the following third parties, some of whom act as data processors while others act as independent data controllers or joint data controllers:
    a. freelance consultants registered in a specific register (lawyers, labour consultants) - for the acquisition of opinions on the correct methods of application of the legislation or for the performance of activities reserved to them by law (legal aid and assistance in court, signing of contracts, etc.);
    b. service providers and platforms for the management of reports and the storage of the data contained therein;
    c. Judicial authority;
    d. Italian National Anti-Corruption Authority (ANAC);

The Data Controller guarantees the utmost care will be taken to ensure that the disclosure of your personal data to the aforementioned recipients concerns only the data necessary to achieve the specific purposes for which they are intended.

Your personal data will not be **disclosed** under any circumstances.

The reports are excluded from the rights of access provided for by Articles 22 et seq. of Law no. 241 of 7 August 1990, and Articles 5 et seq. of Legislative Decree no. 33 of 14 March 2013 (Article 12 of the Decree).

Retention of personal data

The reports and the related documentation are kept, in a form that allows the identification of the data subjects, for the time necessary to process the report and in any case no later than five years from the date of notification of the final outcome of the reporting procedure (Article 14, paragraph 1, of the Decree).

Rights of the data subject

As a data subject, you are granted the rights referred to in Articles 15 to 20 of the GDPR. By way of example, you may:

A. obtain confirmation whether personal data concerning you are being processed or not and, in this case, obtain **access** to the personal data and the following information:
    i. the purposes and methods of processing;
    ii. the identification details of the Data Controller and any data processors;
    iii. the origin of the personal data;
    iv. the categories of personal data in question;
    v. the logic applied in the case of processing carried out with the aid of electronic tools;
    vi. the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular if recipients from third countries or international organisations;
    vii. where possible, the expected retention period of the personal data or, if this is not possible, the criteria used to determine this period;
B. obtain the **rectification** of inaccurate personal data concerning you as well as, taking into account the purposes of the processing, the right to obtain the **supplementing** of incomplete personal data, including by providing a supplementary statement;
C. obtain the **erasure** of your personal data if one of the following reasons exists:
    i. the personal data are no longer necessary with respect to the purposes for which they were

collected or otherwise processed;

ii. the data were processed unlawfully;

iii. you have withdrawn your consent on the basis of which the Data Controller had the right to process your data and there is no other legal basis that allows the Data Controller to carry out the processing;

iv. you objected to the processing and there is no prevailinglawful reason for it to be carried out;

v. the personal data must be deleted to comply with a legal obligation.

Please note that the right to erasure is not exercisable if the processing is necessary for the fulfilment of a legal obligation or for the performance of a task carried out in the public interest or in the exercise of public powers vested in the Data Controller or even if it is necessary for archiving purposes in the public interest, for scientific or historical research or for statistical purposes.

D. obtain from the Data Controller the **limitation** of the processing when one of the following hypotheses applies:

i. for the period necessary for the Data Controller to verify the accuracy of your personal data if you have disputed the accuracy thereof;

ii. in the event of unlawful processing of your personal data;

iii. even if your personal data are not necessary for the purposes of the processing, in any event they must be processed for the establishment, exercise or defence of a right in court;

iv. for the period necessary to verify the possible prevalence of the legitimate reasons of the Data Controller with respect to your request to oppose the processing;

E. to obtain **a certificate** that the operations relating to the rectification,erasure and limitation of the data have been brought to the attention, also with regard to their content, of those to whom the data have been disclosed or disseminated, except in the event that fulfilment of said requirement proves impossible or involves the use of means manifestly disproportionate to the protected right;

Right to object

The Data Subject has the right to object at any time, **for reasons related to their specific situation**, to the processing of personal data concerning them if it is necessary for the performance of a task of public interest or related to the exercise of public powers vested in the Data Controller.

In this case, the Data Controller will refrain from further processing of the personal data unless it proves the existence of compelling legitimate reasons to proceed with the processing that prevail over the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of a right in court. In the case of processing for statistical purposes, the right to object is not exercisable to the extent that the processing is necessary for the performance of a task in the public interest.

Exercise of rights

The person involved or the person referred to in the report, regarding their personal data processed in the context of the report, may not exercise the above rights – for as long as and to the extent that this constitutes a necessary and proportionate measure to ensure the

confidentiality of the identity of the whistleblower - in accordance with the provisions of Article 2-undecies of Legislative Decree no. 196 of 30 June 2003 (Privacy Code).

Right to lodge a complaint with the supervisory authority

Without prejudice to the provisions of Article 2-undecies of Legislative Decree no. 196 of 30 June 2003 (Privacy Code), each Data Subject may lodge a complaint with the Italian Data Protection Authority or with another Supervisory Authority - competent by reason of the provisions of the GDPR - in the event that they consider that their rights pursuant to the GDPR have been violated.

The exercise of the rights of the Data Subject is free of charge.

Changes to the policy

This policy is published and kept updated on the Data Controller's website.

The Data Controller reserves the right to amend, update, add or remove parts of this policy, at its discretion and at any time.

The data subject is required to periodically check for any amendments.

Regulatory sources and additional information

For your convenience, here are the web links where you can find more information (including legal) and news:

a. text of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data repealing Directive 95/46/EC (general data protection regulation) (Text with EEA relevance);
b. website of the Italian Data Protection Authority;
c. website of the European Data Protection Board (EDPB) website (EDPB)