

Information pursuant to Article 13 EU Regulation 679/16 (GDPR)

This notice, made pursuant to Art. 13 GDPR, informs you how we collect, use, share, and store personal data while handling a report of "violations," i.e., conduct, acts, or omissions that harm the public interest or the integrity of the public administration or private entity, as defined by Art. 2, Paragraph 1(a) of Legislative Decree 24/2023.

This information is provided by **Ciam S.p.a., Via Dei Pini, n. 9 Assisi (PG)** as the Data Controller.

What information do we collect, for what purposes, and what are the legal bases?

Although it is optional to provide us with data about you, we inform you that reports, although in the first instance sent anonymously, may later be supplemented with the details of the reporter where necessary to assess the existence of the facts reported, the outcome of the investigation and any measures taken.

Type of data treated

The personal data being processed fall into the following categories:

- Common personal data provided by the reporter, such as biographical data and contact information;
- Judicial data provided by the reporter as governed by Article 10 GDPR;
- Special data provided by the reporter as governed by Article 9 paragraph 2 (g) GDPR;
- Other types of data: information about identified or identifiable individuals, including well-founded suspicions, concerning violations committed or which, based on concrete evidence, could be committed in the organization with which the reporting person or the person making the complaint to the judicial or accounting authority has a legal relationship, as well as elements concerning conduct aimed at concealing such violations.

Purpose of processing

Personal data will be processed for the sole purpose of

- Assess the existence of the reported facts, the outcome of the investigation and any measures taken;
- Provide feedback to the reporting person related to the action taken or intended to be taken on the report;
- Follow up on requests from the relevant administrative or judicial authority and, more generally, public subjects in compliance with legal formalities.

Legal basis of processing

The legal bases for processing appear to be:

Common data

- the need to fulfill a legal obligation to which the Controller is subject (Art. 6(1)(c) GDPR), with reference to the provisions contained:
 - in Legislative Decree 24/2023 (Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019 on the protection of persons

who report breaches of Union law and laying down provisions regarding the protection of persons who report breaches of national laws)

- in Legislative Decree No. 231 of June 8, 2001 ("Regulations on the administrative liability of legal persons, companies and associations, including those without legal personality, pursuant to Article 11 of Law No. 300 of September 29, 2000").
- The reporter's consent (Art. 6(1)(a) GDPR):
 - where, as a result of the use of a recorded telephone line or other recorded voice messaging system, the reporting person's report is documented by the personnel in charge by recording on a device suitable for storage and listening or by verbatim transcription;
 - when, at the request of the reporting person, the report made orally during a meeting with the appropriate personnel is documented by the appropriate personnel by recording on a device suitable for storage and listening or by minutes.
 - in the event that the identity of the reporting person and any other information from which such identity may be inferred, directly or indirectly, are disclosed to persons other than those responsible for receiving or following up reports, who are expressly authorized to process such data;
 - to the disclosure of one's identity, if the disciplinary charge is based, in whole or in part, on the report and the knowledge of the identity of the reporting person is indispensable for the defense of the accused, the report shall be used for the purpose of disciplinary proceedings.

Judicial data

The legal basis for judicial data appears to be identified in Article 10 GDPR with reference to the provisions contained in Legislative Decree 24/2023 (Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019 on the protection of persons who report breaches of Union law and laying down provisions regarding the protection of persons who report breaches of national laws).

Particular data

Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law, which must be proportionate to the purpose pursued, respect the essence of the right to data protection, and provide for appropriate and specific measures to protect the fundamental rights and interests of the data subject (Article 9(2)(g) GDPR).

Confidentiality and protection of the reporter

Pursuant to Article 4 of Legislative Decree 24/2023, the Data Controller has activated its own reporting channels, which guarantee, including through the use of encryption tools, the confidentiality of the identity of the reporting person, the person involved and the person in any case mentioned in the report, as well as the content of the report and the related documentation.

Alerts will not be used beyond what is necessary to adequately follow up on them.

The identity of the reporting person and any other information from which such identity may be inferred, directly or indirectly, may not be disclosed, without the express consent of the reporting person, to persons other than those responsible for receiving or following up reports and expressly authorized to process such data.

Confidentiality and the disciplinary process

Within the scope of disciplinary proceedings, the identity of the reporting person may not be disclosed, where the allegation of the disciplinary charge is based on investigations that are separate and additional to the report, even if consequent to it.

If the charge 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, the report will be usable for the purposes of disciplinary proceedings only if the reporting person expressly consents to the disclosure of his or her identity.

Method of treatment

The Holder has activated its own reporting channels, which guarantee, including through the use of encryption tools, the confidentiality of the identity of the reporting person, the person involved and the person in any way mentioned in the report, as well as the content of the report and related documentation.

Active reporting channels are:

- paper and oral communication
- "Globaleaks" IT platform accessible through the "Whistleblowing" session on the website www.ciamweb.it.

How long do we keep your personal data?

Reports and related documentation shall be retained for as long as necessary for the processing of the report, but no longer than five years from the date of notification of the final outcome of the reporting procedure, subject to confidentiality obligations.

With whom do we share your data?

For the pursuit of the purposes set forth in this Notice, your personal data may be known by persons competent to receive or follow up on reports who are expressly authorized to process such data under Articles 29 and 32(4) of the GDPR, as well as by any Suppliers designated as Data Processors under Article 28 of the GDPR.

The latter will be specifically identified by the Owner, who will also provide special instructions on the methods and purposes of processing and ensure that they are subject to appropriate obligations of confidentiality and privacy.

The management of reporting channels is entrusted:

- to a person specifically trained to manage the reporting channel, identified as Dr. Emanuele Sforna, expressly appointed and authorized to process the data.

The Persons referred to above may also involve Third Parties for the sole purpose of assessing the existence of the facts reported, the outcome of the investigation and any measures taken. Such sharing, if necessary, will take place in compliance with the principles of minimization and proportionality, as well as, where compatible with the purposes of sharing, with the principle of confidentiality of the identity of the reporting person, the person involved and the person in any case mentioned in the report, as well as the content of the report and the related documentation

More generally, the data may be communicated to those to whom the communication must be made in fulfillment of an obligation required by law, regulation or European legislation, or to comply with an order of the Judicial Authority.

Your data will not be disseminated, except in anonymous and aggregate form, for statistical or research purposes.

Data Transfer to Third Countries

We will not transfer your personal data to countries outside the European Economic Area ("EEA"), which includes in addition to the member states of the European Union, Norway, Lichtenstein and Iceland.

In the event that this is necessary to pursue the purposes of the processing operations described in this Notice, our Organization guarantees that all data transfers outside the EEA, if any, will take place in such a way as to ensure the full protection of the rights and freedoms of the data subjects. Where, with respect to the receiving third country no adequacy decisions have been issued by the European Commission, data transfers will be carried out by adopting the safeguards provided for in Articles 46 et seq. of the GDPR including standard contractual clauses approved by the European Commission, and a considered assessment of the legislation of the receiving third country, if any.

Your rights and how to contact us

In your capacity as a data subject, you may exercise your rights under Articles 15 et seq. of the GDPR, namely, the rights to:

- 1) obtain, at any time, confirmation of the existence or otherwise of the processing of the same data and obtain access to personal data and information regarding the processing;
- 2) Request rectification of inaccurate personal data and supplementation of incomplete personal data;
- 3) to request, in the cases indicated by the RGPD, subject to the special regulations provided for certain processing operations, the deletion or limitation of the data, after the prescribed retention periods have elapsed,
- 4) Request portability of your data in accordance with the provisions of the RGPD and national legislation.

Requests should be submitted to DPO@ciamgroup.it.

Right of complaint

If you believe that the processing of personal data relating to you is in violation of the provisions of the Regulations, you have the right to lodge a complaint with the Guarantor, as provided for in Article 77 of the Regulations themselves, or to take appropriate legal action (Article 79 of the Regulations).

Changes

Ciam S.p.a. reserves the right to make changes to this information notice at any time, giving appropriate publicity to the Interested Parties also and guaranteeing in any case an adequate and similar protection of personal data. In order to view any changes, you are invited to regularly consult this policy or contact us at the following e-mail: DPO@ciamweb.it.