

Your data and how to handle a breach report - Whistleblowing Reporting

A brief overview

Transparency first!

We will use your data only to investigate the facts you reported and take any necessary action.

This policy contains all the information regarding the processing of your personal data: where, when, how, and why we process your data, as well as a list of your rights.

Your data will not be transferred to third parties

Your data (i.e. the data you entrust to us) will be used only by Elettrotecnica Rold Srl

If in some cases we use third-party providers, please know that they will operate only on our behalf and in accordance with our instructions.

How to contact us

The data controller is Elettrotecnica Rold Srl, with registered office in Via della Nerviata 1, 20014 Nerviano (MI).

You can contact us at any time by writing to: info@rold.com

Your data and how to handle a breach report - Whistleblowing Reporting

Full disclosure

Last updated: January 24, 2024

Introduction

This notice, provided pursuant to Art. 13 of the GDPR, informs you of how we collect, use, share, and retain personal data when handling a report of "violations," i.e., behaviors, acts, or omissions that harm the public interest or the integrity of a public administration or private entity, as defined in Art. 2, paragraph 1, letter a) of Legislative Decree 24/2023.

This information is provided by Elettrotecnica Rold Srl as the Data Controller.

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

While it is optional to provide us with your personal data, we inform you that reports, even if initially submitted anonymously, may subsequently be supplemented with the reporting party's personal details where necessary to assess the validity of the reported facts, the outcome of the investigation, and any measures taken.

Type of treaties

The personal data processed fall into the following categories:

- Common personal data provided by the reporting party, such as personal details and contact information;
- Judicial data provided by the reporting party as regulated by Article 10 of the GDPR;
- Special data provided by the reporting party as regulated by Article 9, paragraph 2, letter g) of the GDPR);
- Other types of data: information relating to identified or identifiable natural persons, including reasonable suspicions, regarding violations committed or which, based on concrete evidence, could be committed in the organization with which the reporting party or the person filing the complaint with the judicial or accounting authority has a legal relationship, as well as information regarding conduct aimed at concealing such violations.

Purpose of the processing

Personal data will be processed for the sole purpose of:

- assess the existence of the reported facts, the outcome of the investigations and any measures adopted;
- provide feedback to the reporting person regarding the follow-up that is being given or that is intended to be given; report;
- follow up on requests from the competent administrative or judicial authority and, more specifically general, of public entities in compliance with legal formalities.



connected to innovation

Legal bases of the processing

The legal bases for the processing are:

Common data

- the need to fulfill a legal obligation to which the Data Controller is subject (Art. 6, paragraph 1, letter c) GDPR), with reference to the provisions contained therein:
 - or in Legislative Decree 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 reporting breaches of Union law and laying down provisions on the protection of persons reporting breaches of national legislation).
- The consent of the Reporting Person (Article 6, paragraph 1, letter a) GDPR):
 - o in the event that, following the use of a recorded telephone line or another recorded voice messaging system, the reporting person's report is documented by the designated staff by recording it on a device suitable for storage and listening or by full transcription;
 - or when, at the request of the reporting person, the report made orally during a meeting with the relevant personnel is documented by the relevant personnel by recording it on a device suitable for storage and listening or by means of a written report; or in the event that the identity of the reporting person and any other information from which such identity can be deduced, directly or indirectly, are revealed to persons other than those competent to receive or follow up on the reports, expressly authorised to process such data;
 - or to the disclosure of one's identity, if the challenge to the disciplinary charge is based, in whole or in part, on the report and knowledge of the identity of the reporting person is essential for the defense of the accused, the report will be used for the purposes of the disciplinary proceedings.

Judicial data

The legal basis for judicial data is identified in Article 10 of the 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 23 October 2019 on the protection of persons reporting breaches of Union law and laying down provisions regarding the protection of persons reporting breaches of national legislation).

Special data

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

Confidentiality and protection of the whistleblower

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 any person mentioned in the report, as well as the content of the report and related documentation.

Reports 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 can be deduced, directly or indirectly, cannot be revealed without the express consent of the reporting person.



connected to innovation

reporting person, to persons other than those competent to receive or follow up on reports, expressly authorised to process such data.

Confidentiality and disciplinary proceedings

In the context of disciplinary proceedings, the identity of the reporting person cannot be revealed, if the disciplinary charge is based on investigations that are separate and additional to the report, even if they are a consequence of it.

If the complaint is based, in whole or in part, on the report and knowledge of the reporting person's identity is essential for the accused's defense, the report may be used for disciplinary purposes only with the reporting person's express consent to disclosure of their identity.

Treatment methods

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

The active reporting channels are:

IT platform: <https://areariservata.mygovernance.it#!/WB/Rold>

How long do we keep your personal data?

Reports and related documentation are retained for the time necessary to process the report and in any case no longer than five years from the date of communication of the final outcome of the reporting procedure, in compliance with confidentiality obligations.

Who do we share your data with?

In order to pursue the purposes set out in this Policy, your personal data may be disclosed to persons competent to receive or follow up on reports, expressly authorized to process such data pursuant to Articles 29 and 32, paragraph 4, of the GDPR, as well as to any Suppliers designated as Data Processors pursuant to Article 28 of the GDPR.

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

The management of reporting channels is entrusted to:

- to an internal person specifically trained to manage the reporting channel, identified as Daniela Colantropo, belonging to the HR Manager function, in the role of Report Manager;
- to an internal person specifically trained to manage the reporting channel, identified as Claudio Saleri, belonging to the IT function, in the role of Report Manager;
- to an internal person specifically trained to manage the reporting channel, identified as Daniela De Lucia, belonging to the Academy Director function, in the role of Backup Manager.

The above-mentioned Parties may also involve Third Parties for the sole purpose of assessing the existence of the reported facts, the outcome of the investigations, 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 p



connected to innovation

sharing, of the principle of confidentiality of the identity of the reporting person, of the person involved and of the person mentioned in the report, as well as of the content of the report and the related documentation.

More generally, the data may be disclosed to entities to whom the disclosure is required in compliance with an obligation established by law, regulation, or European legislation, or to comply with an order from a judicial authority.

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

Transfer of data 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, Liechtenstein and Iceland.

If necessary to achieve the purposes of the processing described in this Policy, our Organization guarantees that all data transfers outside the EEA will be conducted in a manner that fully protects the rights and freedoms of data subjects. Where no adequacy decisions have been issued by the European Commission with respect to the recipient third-party country, data transfers will be carried out in accordance with the safeguards set forth in Articles 46 et seq. of the GDPR, including the standard contractual clauses approved by the European Commission, and a careful assessment of the legislation of the third-party country of destination.

Your rights and how to contact us

In your capacity as an interested party, you may exercise the rights set forth in Articles 15 et seq. of the GDPR, and specifically, the rights to:

- 1) obtain, at any time, confirmation of whether or not the processing of the same data exists and obtain access to personal data and information regarding the processing;
- 2) request the rectification of inaccurate personal data and the integration of incomplete data;
- 3) request, in the cases indicated by the GDPR, without prejudice to the specific provisions established for certain processing, the deletion or limitation of data, after the expected retention periods have elapsed;
- 4) request the portability of your data in accordance with the provisions of the GDPR and the legislation national.

Requests should be sent to info@rold.com

Right to complain

If you believe that the processing of your personal data violates the provisions of the Regulation, you have the right to lodge a complaint with the Data Protection Authority, pursuant to Article 77 of the Regulation, or to take appropriate legal action (Article 79 of the Regulation).

Changes

Elettrotecnica Rold Srl reserves the right to make changes to this policy at any time, providing appropriate publicity to interested parties and ensuring adequate and similar protection of personal data. To review any changes, you are invited to consult this policy regularly or contact us at the following email address: info@rold.com
