

Data protection information on the whistleblowing system

Information on the processing of personal data in the context of whistleblowing reports

1. What information does this document contain for you?

Below we inform you about the processing of your personal data and your rights as a data subject in the context of the whistleblowing reports.

In doing so, we ensure that we comply with the requirements of the applicable data protection laws (i.e. the EU Regulation No. 2016/679 (GDPR) and the Italian Legislative Decree 196/2003 as amended govern the protection of personal data). Below we provide you with a detailed overview of how we handle your data and your rights.

2. Who is jointly responsible for the processing and who is the data protection officer in each case?

The data controller responsible for processing at thyssenkrupp AG is

thyssenkrupp AG
thyssenkrupp Allee 1
45143 Essen
Phone: +49 201 844-0

You can reach the data protection officer at

E-mail: compliance.gdpr@thyssenkrupp.com

The data controller responsible for processing at thyssenkrupp
Luca Michele Avondetto - luca.avondetto@thyssenkrupp-automotive.com
Stefania Pampolini – Stefania.Pampolini@thyssenkrupp.com
(hereinafter also referred to the “**Data Controller**” or the “**Company**”)

You can reach the data protection officer at

E-Mail: datenschutzbeauftragter@thyssenkrupp.com

The Company bases its data processing on the principles of fairness, lawfulness, transparency and necessity, as provided by in the said legislation. To this end, pursuant to Arts. 13–14 of the GDPR, we provide you with the following information.

3. What categories of data do we process and where do they come from?

We process personal data that you provide to us as part of the whistleblower report or that is collected as part of an investigation. In principle, it is possible to submit reports anonymously and you are not obliged to provide personal data.

The receipt and management of reports leads to the processing of “simple” personal data (first name, surname, job title) of the whistleblower, unless anonymous, and of the person to which the report refers and of any other involved persons, any other information relating to proven or suspected unlawful conduct, and may give rise, depending on the content of the reports and the acts and documents attached to them, to processing of “particular” personal data (relating to health conditions, sexual orientation or trade union membership, pursuant to Art. 9 GDPR) and personal data relating to criminal convictions and offenses (Art. 10 GDPR).

In particular, if you submit a whistleblower report, the following data or data categories, among others, may be processed:

- Master data (e.g. title, surname, first name, gender, date of birth, nationality, photograph, personnel number, 8-ID)
- Salary data
- Contact details (e.g. e-mail address, telephone, fax number, address)
- Business communication data (e.g. content of personal, telephone or written communication)
- Contract data (e.g. contract identifier, contract history)
- Communication data (e.g. content and information on personal, telephone or written communication)
- Bank data, payment data (e.g. payment details, account data, billing information)
- Special categories of personal data, if applicable
- Data on working hours (e.g. recording coming and going)
- Technical data (e.g. log data generated when using our IT systems and machines)
- SAP data (payment release, approval process, order process)
- Data on association memberships (minutes etc.)
- Proof of performance / contracts / proof of payment
- In addition, we process data that we have permissibly obtained from publicly accessible sources (e.g. social or professional networks, land registers, commercial registers, company law links, D&B information) and data that we obtain from public authorities (e.g. search warrants).

4. For what purposes and on what legal basis is data processed?

We collect and process your personal data in compliance with the applicable data protection regulations and all other relevant laws and regulations.

The personal data is collected and processed for the purpose strictly related to the management of reports of misconduct, in violation of national/European rules [and if adopted of the Company's Code of Business Conduct and Ethics, and 231 Model and any other applicable policies], including the conduction of internal compliance investigation for plausibility checks, clarification of misconduct, implementation of legal obligations, taking countermeasures and assertion of legal claims.

In addition, your data will be processed for the purpose of complying with the respective national implementation law for Directive (EU)2019/1937 (EU Whistleblowing Directive).

Taking into account the relevant legislation (the Directive (EU)2019/1937 and the Italian Legislative Decree No. 24/2023 implementing the Directive), your personal data is processed on the basis of the following legal grounds:

- Art. 6 para. 1 lit. c) GDPR:
The fulfilment of a legal obligation to which the Data Controller is subject
- Art. 6 para. 1 lit. f) GDPR:
The legitimate interest of the Data Controller, that consists in the assertion, exercise and defense of legal claims, implementation of legal regulations, implementation and further development of the compliance management system at thyssenkrupp Group.

The provision of the data is necessary for the achievement of the above purposes; failure to provide the data, or providing partial or inaccurate data, may result in the impossibility of handling the report.

5. Who receives your data?

All data is treated as strictly confidential and only made available to persons who are involved in the specific process. This may essentially concern the following group of people:

- Responsible Investigation Compliance Officer
- Responsible Compliance Managers or members of a Collegial Body (e.g. Criminal Compliance Body)
- external companies entrusted with whistleblowing management services and IT service providers (e.g., the IT provider of the whistleblowing platform), which act as Data Processors pursuant to GDPR Art. 28, subject to confidentiality and only for functional purposes of their assignment
- If necessary, the following additional recipients:
 - Other companies in the thyssenkrupp Group
 - Responsible Business Compliance Officer and/or Regional Compliance Officer

- Internal employees of other corporate functions involved such as Internal Auditing (AUD), Human Resources (HR) etc.
 - External employees of involved service providers (law firms and auditing firms)
- The Company's Supervisory Body (OdV), if any
- Employees at the level of the Group companies, business units or business segments involved
- Law enforcement, financial and other public authorities fulfilling specific legal obligations and judicial authorities acting as independent data controllers.

6. What processing methods are used?

The data provided within the framework of the report will be processed mainly by electronic and manual systems in accordance with the principles of fairness, loyalty and transparency laid down by the applicable legislation on the protection of personal data and by the provisions on whistleblowing, protecting the confidentiality of the person to whom the data refer and adopting technical and organisational security measures to ensure an adequate level of security (e.g. preventing access to unauthorised persons except in cases required by law, or the ability to restore access to the data in the event of physical or technical incidents).

The identity of the whistleblower and any other information from which such identity can be derived, directly or indirectly, shall be processed exclusively by persons authorized to process data pursuant to GDPR Article 29 and shall not be disclosed to other persons without the whistleblower's specific consent, as prescribed by Article 12(2) of the Decree. Consent is voluntary and is given at the time of reporting via the platform.

7. How long will your data be stored?

Reports and related documentation (including any recordings, if a recorded telephone line or other recorded voice messaging system is used for reporting) shall be retained, in accordance with the principle of minimization, for the time necessary to process the report and in any case no longer than 5 years from the date of communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations laid down in the relevant legislation in force, except in the event of specific requirements to defend or protect the rights and/or legitimate interests of Data Controller or third parties, including in the event of complaints, litigation or pre-litigation. At the end of the retention period, we delete the records.

Personal data that are clearly not useful for the processing of a specific report shall not be collected or, if accidentally collected, shall be deleted promptly.

8. Will your data be transferred to a third country?

In principle, your data will not be transferred to a third country outside the European Economic Area. In exceptional cases, the transfer of your data to third countries to affected group

companies or involved authorities may be necessary for the proper conduct of an internal compliance investigation. In these cases, the Data Controller undertakes to ensure adequate levels of protection and safeguards, including contractual safeguards, in accordance with the applicable regulations, including the stipulation of standard data protection contractual clauses (see Art. 46 (2) lit. c) GDPR).

You can request further information on this by using the contact information above.

9. What data protection rights can you assert as a data subject?

You have the right to request information about the personal data stored about you, Art. 15 GDPR. In addition, you can request the rectification or erasure of your data, Art. 16, 17 GDPR. You may also have the right to restrict the processing of your data and the right to receive the data you have provided in a structured, commonly used and machine-readable format, provided that this does not adversely affect the rights and freedoms of others, Art. 18, 20 GDPR.

If you have given us your consent to process your personal data, you can withdraw this consent at any time with effect for the future. This shall not affect the lawfulness of processing based on consent before its withdrawal.

You also have the right to object, which is explained in more detail at the end of this data protection notice.

You also have the option of lodging a complaint with a Italian Data Protection Authority (Art. 77 GDPR) at Piazza Venezia 11, 00187 Rome, Italy.

If you have any further questions about any privacy matters, or if you wish to exercise your rights, please contact the Data Protection Officer named in section 2.

Information about your right to object in accordance with Art. 21 of the General Data Protection Regulation (GDPR)

You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on point (f) of Article 6(1) GDPR (data processing based on a weighing of interests); this also applies to any profiling based on this provision within the meaning of Article 4(4) GDPR.

If you object, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defense of legal claims.

If you object to processing for direct marketing purposes, we will no longer process your personal data for these purposes.

Information pursuant to Art. 26 para. 2 GDPR on joint responsibility:

The joint responsibility of the parties applies to the operation and organization of the whistleblower system within the thyssenkrupp Group. This includes the internal administration of the whistleblower system and the implementation of whistleblower procedures. The parties use a uniform compliance management system and uniform IT systems for this purpose. The parties have agreed that data subjects can assert their data protection rights directly against thyssenkrupp AG using the contact details given above. Data subjects may nevertheless exercise their rights against any jointly responsible party.

This privacy notice has been updated on 30/06/2026

The Data Controller