Privacy notice (data protection information on the whistleblowing system)

Information on the processing of personal data in the context of the whistleblowing system follows below as per the EU's General Data Protection Regulation (Regulation 679/2016) ("GDPR") and Hungarian law, including Act no. XXV of 2023 on Complaints and Reports of Public Interest and the Rules of the Handling of Reports of Abuses ("Whistleblowing Act") transposing the 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.

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 within the context of the whistleblowing system.

In doing so, we ensure that we comply with the requirements of the applicable data protection laws. Below we provide you with a detailed overview of how we process your personal data and how we ensure your rights.

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

The controller responsible for processing is thyssenkrupp Materials Hungary Zrt If the report is made directly to thyssenkrupp Materials Hungary Zrt and the company does not share the report with the compliance department of thyssenkrupp AG (CO/L&C-INV) as described in the whistleblowing policy (see Section 4 of Part "How can a report be submitted?"), then thyssenkrupp Materials Hungary Zrt is a sole controller.

The contact details of the data protection officer of thyssenkrupp Materials Hungary Zrt. is: Kamarás Viktor, viktor.kamaras@thyssenkrupp-materials.com, 1158 Budapestr, Fázis str. 6., Hungary

If the whistleblower makes the report directly to the compliance department of thyssenkrupp AG (seat: thyssenkrupp Allee 1, 45143 Essen, Germany) or thyssenkrupp Materials Hungary Zrt shares the received report with the compliance department of thyssenkrupp AG as per Section 4 of Part "How can a report be submitted?" of the whistleblowing policy, then thyssenkrupp Materials Hungary Zrt and thyssenkrupp AG qualify as joint controllers for the purposes of conducting the internal investigation.

The contact details of the data protection officer of thyssenkrupp AG are:

E-mail: compliance.gdpr@thyssenkrupp.com
Address: compliance department (CO/L&C-INV), thyssenkrupp Allee 1, 45143 Essen, Germany

Further information on the essence of the joint controllership agreement is detailed below at the end of this privacy notice.

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

We process personal data the whistleblower provides to us in their report and data collected as part of an investigation. It is possible to submit reports anonymously and the whistleblower is not obliged to provide personal data. If a report is submitted, depending on the content of the report, amongst others, the following data or data categories may be processed to the extent absolutely necessary for the proper investigation of the report:

- Personal data including (e.g. title, surname, first name, gender, date of birth, nationality, photograph, personnel number)
- Contact details (e.g. email 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)
- 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. working hour registry)
- Technical data (e.g. log data generated when using our IT systems and devices)
- SAP data (payment release, approval process, order process)
- Data on association memberships (minutes etc.)
- Proof of performance / contracts / proof of payment
- Data obtained during interviews with persons who have or may have a material knowledge about the potential wrongdoing reported
- Data we can lawfully obtain from publicly accessible sources (e.g. social or professional networks, land registers, commercial registers) and data received from public authorities.

Under the Whistleblowing Act, within the framework of the whistleblowing system, personal data
a) of the whistleblower,
b) of the person whose conduct or omission gave rise to the report, and
c) of the person who may have substantial information of the matter to which the report relates,

which personal data are essential to the investigation of the report may be processed only for the purposes of investigating the report and remedying or stopping the conduct that is the subject of the report and may be disclosed to a whistleblower protection lawyer or to an external organisation involved in the investigation of the report.

The whistleblower is requested to provide only such data which are necessary for making the report. Any personal data submitted and not necessary for the investigation of the report will be deleted without delay.

Source of personal data:

Within the context of an internal investigation, we process personal data received from the whistleblower and personal data received from other sources (e.g. persons who have or may have a knowledge of the reported potential wrongdoing, publicly available sources and/or authorities/courts).

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

Purpose of processing:

thyssenkrupp Materials Hungary Zrt is obliged to set up an internal reporting system pursuant to Section 18 of the Whistleblowing Act, given that the number of the company's employees exceeds 49. The company has set up the internal reporting system in compliance with this legal obligation, in which personal data will necessarily be processed upon receipt of a report. The purpose of the processing is to enable the company to comply with its legal obligation to establish and operate an internal whistleblowing system under the Whistleblowing Act, to investigate the reports received and to take appropriate action. Likewise, where joint processing takes place with thyssenkrupp AG, the purpose of processing is the same, i.e. to investigate the reports received and take appropriate action.

In other words, the personal data is processed for the purposes of conducting internal compliance investigations as per and complying with the provisions of the Whistleblowing Act and applicable laws. The purpose of the investigations is to identify or disprove conduct potentially relevant to regulatory and criminal law and to identify or disprove violations of internal compliance guidelines. Personal data is processed in particular for examination of the report received, clarification of misconduct, implementation of legal obligations, the taking of countermeasures and the assertion of legal claims.

The personal data is processed on the basis of the following legal bases:

- Fulfilment of the company's legal obligation (Art. 6 para. 1 lit. c) of the GDPR) in conjunction with Sections 18-28 of the Whistleblowing Act serves as legal basis of processing (where examination of the report is a must and may not be waived as per the Whistleblowing Act).

If special categories of data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons) are processed, the legal basis of the processing is the company's legal obligation (Article 6(1)(c) of the GDPR and Sections 18-28 of the Whistleblowing Act), and the processing is further subject to Article 9(2)(b) of the GDPR (processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment), Article 9(2)(f) (processing is necessary for the establishment, exercise or defence of legal claims) and Article 9(2)(g) (processing is necessary for reasons of substantial public interest) of the GDPR.

- Where the company is not obliged to investigate the report under the Whistleblowing Act, the company's and thyssenkrupp AG's legitimate interest (Art. 6 para. 1 lit. f) GDPR) serves as legal basis of processing. This is the case if (i) the report has been made by a person who cannot be identified, (ii) a person other than those listed in Section 1 of Part "Scope" of the whistleblowing policy makes a report, (iii) the report is a repeated application by the same whistleblower with the same content as the previous report, (iv) the harm to the public interest or to an overriding private interest would not be proportionate to the restriction of the rights of the natural or legal person resulting from the investigation of the report, or (v) if thyssenkrupp AG is involved in the investigation.
  The legitimate interest consists of the assertion, exercise and defense of legal claims, being able to investigate a report, also if the potential wrongdoing may have a serious negative effect also on thyssenkrupp AG and/or the thyssenkrupp group, and the implementation of legal regulations.
  If special categories of data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons) are processed, the legal basis of the processing is the company's and thyssenkrupp AG's legitimate interest (Art. 6 para. 1 lit. f) GDPR and being able to implement Articles 18-28 of the Whistleblowing Act), and the processing is further subject to Article 9(2)(f) (processing is necessary for the establishment, exercise or defence of legal claims) and Article 9(2)(g) (processing is necessary for reasons of substantial public interest) of the GDPR.

5. Who receives the personal data processed?

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

- System Manager at the company and a contracted external legal advisor, if the report is made to the company,

- The compliance department of thyssenkrupp AG if the report is made to thyssenkrupp AG,
- If necessary, the System Manager may share the report with the compliance department of thyssenkrupp AG,
- If necessary, the following additional recipients: service providers (law firms, auditing firms and IT service providers); e.g. external legal advisor retained by thyssenkrupp Materials Hungary Zrt and/or thyssenkrupp AG with a view to seeking legal advice as to the assessment and handling of the report,
- If necessary, law enforcement, financial and other authorities.

The internal whistleblowing system is designed in such a way that the personal data of the whistleblower who discloses his/her identity and of the person concerned by the whistleblower's report (i.e. the person against whom the report is made and any person who may have a material knowledge about the facts reported) may not be disclosed to persons other than those entitled to have such data. Pending the conclusion of the investigation or the initiation of formal prosecution as a result of the investigation, the persons investigating the report may, in addition to informing the person concerned, share information on the content of the report and the person concerned with other departments or staff of the employer only to the extent strictly necessary for the conduct of the investigation.

Where it has become apparent that the whistleblower has communicated false data or information in bad faith and
a) the circumstances suggest that a criminal offence or offence has been committed, the whistleblower's personal data must be handed over to the body or person entitled to conduct the proceedings,
b) there are reasonable grounds for believing that the whistleblower has caused unlawful damage or other harm to another person, the whistleblower's personal data must be handed over to the authority or person entitled to initiate or conduct the proceedings, at the latter's request.

The personal data of the whistleblower may, except as provided for in the previous paragraph, be disclosed only to the body competent to conduct the proceedings initiated on the basis of the report, if such body is entitled to process the data by law or if the whistleblower has consented to the disclosure of the data. The personal data of the whistleblower may not be published without their consent.

6. How long will your data be stored?

If the investigation initiated on the basis of the report establishes the infringement of employment law, the law of offences, any criminal offence or any other infringement on the basis of which the employer issues a warning to the employee or takes disciplinary proceedings (including the termination of the employment relationship), the data will be deleted after 5 years from the closing of the investigation.

If the investigation initiated on the basis of the report establishes the infringement of employment law, the law of offences, any criminal offence or any other infringement on the basis of which court proceedings or other official proceedings are initiated, the data will be processed until the final conclusion of the proceedings initiated/started.

If, as a result of the investigation, it is established that no infringement has occurred and no disciplinary, official or judicial proceedings are initiated, the data will be processed in connection with the investigation for a maximum period of 12 months after the investigation is closed, after which the data will be deleted.

If the controller decides in a way that the report will not be investigated (see the last paragraph of Section 1 of Part "Scope" of the whistleblowing policy), the report will be deleted, including the data contained therein, immediately after the decision not to investigate the report is made.

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

As a rule, no personal data will be transferred to a third country (i.e. a country outside the EU/EEA). In exceptional cases, the transfer of personal data to third countries to affected group companies may be necessary for the proper conduct of the internal investigation of the report. In these cases, the appropriate level of protection will be ensured by using standard data protection clauses as approved by the European Commission (see Art. 46 (2) lit. c) GDPR). Depending on the data protection status of the recipient (controller or processor), the respective standard contractual clauses will be used. Information on the standard contractual clauses are available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en and https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. You can request further information on this by using the contact information above. Also, necessary additional measures as required by the practice of the CJEU will be duly applied. At the same time, the data processed within the whistleblowing system may be transferred to a third country (or an international organisation) only if the recipient of the transfer has made a legal undertaking to comply with the rules on reporting set out in the Whistleblowing Act and subject to the provisions on the protection of personal data.

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

You have the right to request information about the personal data processed about you (Art. 15 GDPR). Under the Whistleblowing Act, if the report relates to a natural person, during the exercise of the right of information and access to personal data of that natural person under the provisions on the protection of personal data, the personal data of the whistleblower may not be disclosed to the person requesting the information (the person against whom the report was made may not get access to the personal data of the whistleblower).

In addition, you can request the rectification or erasure of your data (Art. 16 and 17 GDPR). For example, you may request the rectification of your data if the data processed is inaccurate and may request the completion of any incomplete data. Also, for example, you may request the deletion of your data if e.g. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, or if you object to the processing and there are no overriding legitimate grounds for the processing.

You may also have the right to restrict the processing of your data (Art. 18 GDPR). This is the case if e.g. you contest the accuracy of the personal data and the controller has to verify the accuracy of the personal data, or if you have objected to processing when the controller has to verify whether the legitimate grounds of the controller override your rights.

You also have the right to receive the data you have provided in a structured, commonly used and machine-readable format where your consent serves as the processing of your personal data, provided that this does not adversely affect the rights and freedoms of others (Art. 20 GDPR).

If you have given us your consent to process your personal data (for making of voice recording or for the publication of 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 privacy notice.

To exercise the above rights, please contact any of the controllers or data protection officers named in section 2 above.

You have the right to lodge a complaint with a supervisory authority (Art. 77 GDPR), in particular in the Member State of your habitual residence, place of work or place of the alleged infringement, if you consider that the processing of personal data concerning you infringes data protection law. In Hungary, complaints can be made to the National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa u. 9-11; telephone: +36 1 391 1400; fax: +36 1 391 1410; postal address: 1363 Budapest, Pf.)

You also have the right to take legal action if you believe that your rights have been infringed as a result of the processing of your personal data in breach of the law. Proceedings against the controller must be brought before the courts of the Member State where the controller is established, but may also be brought before the courts of the Member State where you are habitually resident (Art. 80 GDPR).

No automated decision-making will take place.

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 to

processing, you are kindly requested to elaborate on your particular situation, i.e. why you are objecting to processing.

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.

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

The joint responsibility of the controllers arises, i.e. joint controllership takes place if (i) the whistleblower has submitted the report relating to thyssenkrupp Materials Hungary Zrt to the compliance department of thyssenkrupp AG (because the whistleblower suspected that there may be a conflict or the impartiality of the investigation would be endangered if the report was made to thyssenkrupp Materials Hungary Zrt or (ii) the report concerns a matter which could potentially have a negative effect on thyssenkrupp AG and the company shares the report with the compliance department of thyssenkrupp AG (e.g. in potential competition law violations, like cartelling). This includes the joint internal investigation of such reports within the whistleblowing system. The parties have agreed that data subjects can assert their data protection rights directly against either thyssenkrupp Materials Hungary Zrt or thyssenkrupp AG using the contact details given above.

Status: 2025