PRIVACY NOTICE

on the operation of a whistleblowing system

A **thyssenkrupp Components Technology Hungary Korlátolt Felelősségű Társaság** (registered seat: 1117 Budapest, Budafoki út 56.; company registration number: 01-09-887088; „**TKHU**" or „**Employer**" or „**we**"), as an employer according to § 18 (1) of Act XXV of 2023 on Complaints and Public Interest Disclosures, and on the Rules of Whistleblowing Notifications ("**Whistleblowing Act**"), operates a whistleblowing system for the reporting of unlawful or allegedly unlawful acts or omissions or other including other cases of misuse. TKHU **processes personal data** in the course of the operation of the whistleblowing system.

In this privacy notice ("**Notice**") TKHU informs you about the processing of your personal data regarding the operation of the whistleblowing system pursuant to Articles 13-14 of the General Data Protection Regulation 2016/679 of the European Parliament and of the Council (hereinafter "**GDPR**").

The scope of this Notice covers all data processing concerning the reporting, investigation and handling of reports to the whistleblowing system operated by TKHU, regardless of the capacity in which the reporting person (e.g. employed person, person under contract with TKHU[1]) reports to the whistleblowing system.

This Notice is published as set out in clause 1.3 of the internal whistleblowing policy of thyssenkrupp Components Technology Hungary Korlátolt Felelősségű Társaság and, in the case of lodging a report, it is also sent directly to the data subjects about whom the report contains personal data (reporting person, person concerned by the report, witness or third party). In exceptional and justified cases, the person concerned by the report may be informed at a later stage if immediate information would prevent the investigation of the report.

We may update or change this Notice in the event of any changes to the processing of data under this Notice. In such a case, we will also publish the updated Notice by means considered customary locally.

The terms used in this Notice have the meaning given in Article 4 of the GDPR.

1. Name and contact details of the data processor

Data controller is the person or company that processes the data in any way: for example, storing, copying, saving, transmitting, erasing.

The personal data provided will be processed by TKHU. The contact details of TKHU are:

name: ***thyssenkrupp Components Technology Hungary Kft.***
registered office: 1117 Budapest, Budafoki út 56.
company registration number: 01-09-887088
phone: +36 1 505-9100
fax: +36 1 505-9101
website: www.thyssenkrupp.hu
email address: info.hun@ thyssenkrupp-automotive.com

2. Name and contact details of the data protection officer

TKHU is not obliged to appoint a data protection officer under Article 37 of the GDPR and no data protection officer has been appointed.

[1] For a list of other persons entitled to make a report, see section 4 of the *thyssenkrupp Components Technology Hungary Limited Liability Company's internal whistleblowing policy* https://www.thyssenkrupp.hu/en/whistleblowing

3. Categories and source of personal data

TKHU processes the following categories of personal data:

- ***Master data***[2] : your name and address;

- ***Contact details****:* your contact details, as you have chosen (address, e-mail address, telephone number),

- ***Communication data (including data shared on communication platforms):*** the content of the communication with you, the circumstances of the communication (in particular, the names of the parties involved, date/time and duration);

- ***Data included in the report***: any personal data provided by the reporting person in the report, including, but not limited to, the following personal data: master data, contact details (for the list of specific personal data, see above), personal data relating to the relationship between the Employer and the reporting person, personal data relating to the history of the report (if any), data and statements relating to the circumstances supporting the good faith of the report, identification of the person concerned by the report, identification of other persons, personal data relating to the conduct complained of or the description of the event described in the report, indication of the circumstances, personal data contained in any evidence attached, date of the report, signature of the reporting person;

- ***Protocol data***:

  (i) the protocol data of *the hearing held in connection with the investigation*: place, date and starting time of the hearing, names and positions of the persons present, indication of the relationship with the Employer and/or the circumstances establishing the right to report, the capacity in which the person concerned by the report is participating in the hearing, the subject of the hearing, the questions asked and the answers given during the hearing, other statements made by the person interviewed and the personal data contained therein, the fact of the presentation of the protocol, any comments or statements of agreement made thereon, the closing time of the recording of the protocol, the signatures of the persons present during the hearing;

  (ii) *personal data recorded in the protocol of report lodged by telephone or personal meeting*: name of the reporting person, job title, Contact details (see above), indication of the relationship with the Employer and/or the circumstances establishing the right to report, the data included in the report (see above), the reporting person's other statement, as well as the personal data included in it, the name and job title of the person recording the protocol, the fact that the content of the protocol was disclosed, any comments or agreement given thereon, the start and end date, place and date of recording the protocol, signature of the person taking the protocol and other persons present;

- **Final report data**: personal data contained in the final report on the outcome of the investigation, the action taken in the course of the investigation and the measures deemed necessary by the investigator.

We have received the personal data from you as the data subject, or the personal data has been disclosed to us by the reporting person or other person who has cooperated with the investigation (e.g. a witness).

[2] In relation to a reporting person only if the reporting person has not made the report anonymously.

Purpose and legal basis for the data processing

TKHU processes the personal data specified in clause 3 above for the following purposes and on the following legal basis:

#	Purpose of data processing	Data processed	Legal basis for processing
3.2	**Operating a whistleblowing system, receiving reports**	Master data; Contact details; Communication data; Data contained in the report; Protocol data of telephone or personal reporting	Legal obligation (Article 6 (1) c) GDPR)
3.3	**Investigating reports** **Including: holding any hearings, assessing the evidence provided by the reporting person, communicating with the reporting person, the person concerned by the report or a third party (e.g. a witness), informing the reporting person and the person concerned by the report in connection with the report, its investigation and the conclusion of the investigation and the measures taken, making accusations, report to authorities, if such action appears to be justified on the basis of the report**	Master data; Contact details; Communication data; Data contained in the report; Protocol data	Legal obligation (Article 6 (1) c) GDPR)
3.4	**Further measures to be taken according to the results of the investigation**	Master data; Data contained in the report; Protocol data Final report data	Employer's legitimate interest (GDPR Article 6 (1) f)) *It is in the legitimate interest of the Employer* to take the necessary measures (e.g. labour law measures, ordering a further internal investigation) based on the results of the investigation.

If the reporting person also provides TKHU with personal data belonging to a special category of personal data and the personal data is necessary for the investigation of the report, therefore, such data cannot be erased, the processing of such data by the TKHU is necessary for reasons of substantial public interest on the basis of EU or Member State law (Article 9 (2) g) GDPR). Except for the case specified in clause 3.4 in which the processing of the personal data carried out by TKHU is necessary for the establishment, exercise or defence of legal claims (Article 9 (2) f) GDPR).

4. Persons entitled to access the data

(a) Internal recipients (within TKHU)

Only to those persons have access to the personal data under this Notice to whom the access is strictly necessary for the investigation of the report or for making other decision related to the report or for the provision of the IT system.

Accordingly, the following persons may have access to the personal data processed in the course of the operation of the whistleblowing system:

Job title / division / department	**Purpose of access**	**Personal data processed**
Whistleblower Protection Officer	Handling and investigating a report, informing the reporting person and the person concerned, contacting the reporting person	All personal data referred to in point 3
Managing Director of TKHU	Receiving summary reports and deciding on the measure proposals contained therein	All personal data referred to in point 3
Person involved in the execution of a measure on the basis of the report	Execution of measures to be taken on the basis of the investigation of a report	Personal data necessary for the execution of measures
IT	IT system provision	Personal data necessary for the execution of IT measures

(b) External recipients (outside TKHU)

Except as provided for in this point, the personal data of the reporting person may be disclosed only to the body competent to carry out the procedure initiated on the basis of the report, if that body is entitled to process the data by law or if the reporting person has consented to the disclosure of the data. The personal data of the reporting person shall not be disclosed without his consent.

If it has become apparent that the reporting person has communicated false data or information in bad faith and

(a) where there are indications that a criminal or administrative offence has been committed, the personal data must be transferred to the authority or person responsible for the procedure,

(b) there are reasonable grounds for believing that the reporting person has caused unlawful damage or other legal harm to another person, the personal data must be disclosed to the body or person entitled to initiate or conduct the proceedings, at the request of that person.

In addition, the name and address or notification address of the reporting person may also be transferred to a postal service provider, courier service, parcel service, acting as a separate data controller, if the processing of TKHU would require the transmission of letters, parcels, packages, etc.

5. Transfer of personal data to a third country

No transfer of personal data to third countries will take place.

6. Automated decision-making, including profiling

No automated decision-making or profiling will take place.

7. Data retention period

Scope of data	**Erasure deadline**
Reports and personal data contained therein which are **not suitable for investigation**	erased or anonymised within 8 working days as of receipt at the latest
reports and personal data contained therein, which **we will omit to investigate pursuant to § 22 (6) of the Whistleblowing Act**	erased or anonymised within 8 working days of receipt
personal data contained in the report which are **not strictly necessary for the investigation of the report**	erased or anonymised within 8 working days of receipt
Substantially (content based) investigated report and the personal data contained therein, if **no further measure is taken** on the basis of the result of the investigation	erased or anonymised within 30 working days of the end of the investigation of the notification, which will take 30 days up to a maximum of 3 months
Substantially (content based) investigated report and the personal data contained therein, if **further measure is taken** on the basis of the result of the investigation	the personal data will be kept for the duration of the further measure and will be deleted or anonymised within 5 years, or in the case of an employment measure 3 years, commencing at the end of the year in which the measure is executed
In the event of a **dispute following a report or further measure**	the personal data will be erased or anonymised within 30 working days as of the final resolution of the dispute or the expiry of the limitation period for bringing a claim (3 years in the case of an employment claim, 5 years in the case of a civil claim, or the maximum period of the criminal penalty, but not less than 5 years in the case of a criminal claim)

8. Consequences of failure to provide data

If case you do not provide your Master Data, we are not obliged to investigate your report.

If you do not provide us with the other information we need to investigate your report, despite a request for a deficiency report, we will not be in a position to investigate your report.

9. Your rights as a data subject concerned

- You can request TKHU for

a) **access to your personal data** (Article 15 GDPR).In this regard, you are entitled to obtain information as to whether or not your personal data are being processed, and access the personal data (including obtaining copies) and information relevant from a data protection perspective (e.g. categories of recipients, storage period, safeguards relating to international data transfers, etc.).

b) **rectification of** your personal data (Article 16 GDPR). In this regard, you are entitled to rectification of incorrect data or the completion of incomplete data.

c) **erasure of** your personal data (Article 17 GDPR) or

d) **restriction of processing** of your personal data (Article 18 GDPR).

- You have the **right to object** against the processing of TKHU based on legitimate interests (cf. clause 0.) on grounds relating to your own situation. If you wish to exercise your right of objection under this point, please also indicate in your request the ground relating to your personal situation on which you establish your right of objection.

- Request for enforcement of abovementioned rights may be lodged to TKHU on the contact details in clause 1. TKHU shall fulfil the application as soon as possible, but not later than 10 days, and will inform you of the measures taken or the reasons for the refusal of the application.

- **Right to lodge a complaint**: you have the right to lodge a complaint with the Hungarian National Authority for Data Protection and Freedom of Information (1055 Budapest, Falk Miksa utca 9-11.; website: www.naih.hu; email: ugyfelszolgalat@naih.hu; Tel: + (36)-1-391-1400). Before submitting your complaint to the Authority, you are recommended to submit such complaint to TKHU so that we can investigate your request first.

- **Judicial remedy**: in the event of an infringement of your rights you are entitled to seek judicial remedy against TKHU. Ruling in the matter falls under the jurisdiction of the regional court. Actions may be brought, at your option, before the competent regional court where you are living or residing.

In the course of exercising the right of information and access of personal data of person concerned by the report, the personal data of the reporting person shall not be disclosed to the person requesting the information.