Privacy information

We take the issue of data protection and confidentiality very seriously and follow the provisions of the EU General Data Protection Regulation (“GDPR”) as well as applicable national data protection regulations. Please read this data protection information carefully before submitting a report.

Purpose of the processing and legal basis

The reporting system is used to receive, process and manage information on compliance violations in a secure and confidential manner. The processing of personal data as part of the reporting process is based on the legitimate interest of our company in the detection and prevention of wrongdoing and thus in the prevention of damage to the controller, its employees and customers. The legal basis for this processing of personal data is Article 6 (1) lit. f GDPR.

The processing of the reporting party's identification data is based on consent to be given (Art. 6 (1) lit. a GDPR). The voluntary nature of the consent is given by the fact that the notice can also be given anonymously instead. However, the revocation of consent can generally only take effect within one month after the report has been made, as the controller is obliged in certain cases under Art. 14 (3) lit. a GDPR to inform the accused person of the allegations made against him or her and the investigations carried out within one month, including the storage, the type of data, the purpose of the processing and the identity of the controller and, if applicable, the whistleblower, and it is then no longer possible to stop the data processing of the whistleblower's identification data. In addition, the processing of the data has already progressed so far after that point that deletion is no longer possible. However, the revocation period may also be shortened, sometimes considerably. This is the case if the nature of the notification requires the immediate involvement of an authority or a court. As soon as we have disclosed the name to the authority or court, it is in our procedural files as well as with the authority or court and can no longer be deleted.

Data controller

The data controller for data protection is:

Controller: Wethje Carbon Composites GmbH, Donaustraße 35, 94491 Hengersberg

The reporting system is operated by a specialist company, Safecall Limited, Loftus House, Colima Avenue, Sunderland SR5 3XB, United Kingdom ("Safecall"), on behalf of the data controller.

Personal data and information entered into the reporting system are stored in a database operated by Safecall in a high-security computer centre in the United Kingdom. The inspection of the data is only possible for a limited group of employees of the data controller. This is ensured in a certified procedure by comprehensive technical and organisational measures.

All data is encrypted and stored with multiple levels of password protection, so that access is limited to a very narrow circle of recipients who are expressly authorised.

Data Protection Officer

The data controller has appointed a data protection officer. Data subjects can contact the data protection officer directly:

TÜV Technische Überwachung Hessen GmbH
Business Assurance Geschäftsfeld Data Protection & Information Security
Robert-Bosch-Str. 16 64293 Darmstadt
Nicolas Kurze (Nicolas.Kurze@tuevhessen.de)

Type of personal data collected

Use of the reporting system is on a voluntary basis. When you submit a report via the reporting system, we collect the following personal data and information:

- your name, provided you disclose your identity,
- your contact details, if you provide them
- that you have submitted a report via the reporting system
- whether you are employed by the data controller and

where applicable, names of persons and other information and personal data of the persons you name in your notification.

Confidential treatment of information

Incoming information is received by a narrow circle of expressly authorised and specially trained employees of the Compliance Organisation of the responsible party and is always treated confidentially. The employees of the Compliance Organisation examine the facts of the case and, if necessary, carry out a further case-related clarification of the facts.

Any person who gains access to the data is obliged to maintain confidentiality.

Data transmission

In the course of processing a report or in the course of a special investigation, it may be necessary to pass on information to other employees of the person responsible or employees of other group companies, *e.g.* if the information relates to events in a subsidiary.

In addition, your personal data will be forwarded to third parties or authorities in individual cases for further investigations if it is necessary to clarify unlawful conduct or for legal prosecution. However, this only happens if there are concrete indications of unlawful or abusive behaviour.

The disclosure of this data is based on our legitimate interest in combating abuse, prosecuting criminal offences and securing, asserting and enforcing claims, unless your rights and interests in the protection of your personal data are overridden, Art. 6 para. 1 lit. f GDPR. If we are obliged to disclose this information under the laws of the member states, the disclosure is made on the basis of Art. 6 para. 1 lit. c) GDPR.

The above-mentioned groups of recipients may also be based in countries outside the European Union or the European Economic Area, in which different regulations for the protection of personal data may exist. We always ensure that the relevant data protection regulations are complied with when passing on information.

Information of the accused person

In accordance with Art. 14 of the GDPR, we are legally obliged to inform third parties that we have received a tip-off about them and that we are processing your personal data as soon as this information no longer jeopardises the follow-up of the tip-off. Your identity as a whistleblower will not be disclosed - as far as legally permissible.

Confidentiality cannot be guaranteed if false information is knowingly posted with the aim of discrediting a person (denunciation).

Data subjects' rights

According to GDPR, you and the persons named in the notice have the right to information, correction, deletion, restriction of processing and the right to object to the processing of your personal data. If the right of objection is exercised, we will immediately check the extent to which the stored data is still required for the processing of a notice. Data that is no longer required will be deleted immediately. You also have the right to lodge a complaint with the competent supervisory authority.

Retention period of personal data

Personal data will be stored as long as it is required for the clarification and final assessment of the information or if there is a justified interest of the company or if this is required by law. After the processing of the information has been completed, this data is deleted in accordance with the legal requirements.

Use of the reporting system

Communication between your computer and the reporting system takes place via an encrypted connection (SSL). The IP address of your computer is not stored during the use of the reporting system. To maintain the connection between your computer and the reporting system, a cookie is stored on your computer that only contains the session ID (so-called zero cookie). The cookie is only valid until the end of your session and becomes invalid when you close your browser.

You can securely send reports to the responsible staff member by name or anonymously. With this system, the data is stored exclusively in the reporting system and is therefore particularly secure; it is not an ordinary e-mail communication. You will be assigned an individual code per report. For more details, please visit the Safecall's data processing terms at Data Processing Schedule (safecall.co.uk).

Notes on sending attachments

When submitting a report or sending a supplement, you have the option of sending attachments to the responsible officer. If you wish to submit a report anonymously, please note the following security advice: Files may contain hidden personal data (so-called metadata, *e.g.* by whom the file was last saved) that endanger your anonymity. Remove this data before sending. If you are unable to remove this data or are unsure, copy the text of your attachment to your message text or send the printed document anonymously using the reference number you will receive at the end of the message process.