What is "*Whistleblowing*"?

Whistleblowing means the act of reporting a wrongdoing.

Mitsubishi Chemical Group EMEA ("MCG EMEA") and whistleblower information and protection

Within the EMEA region, in accordance with the so-called Whistleblower Directive[1], and the national laws implementing it, MCG EMEA has established safe channels to protect whistleblowers.

MCG EMEA has a non-tolerance policy regarding retaliation against good faith whistleblowers.

I. Who can be a whistleblower?

Any person can be a whistleblower. whistleblowers are persons who have obtained information in connection with their professional activities about actual or potential misconduct and want to report it, such as:

- Employees, including those whose employment relationship has already ended, job applicants, trainees, temporary workers;
- Self-employed persons providing services, freelancers, contractors, subcontractors, suppliers, business partners and their employees;
- Shareholders and persons on governing bodies;
- Any third parties, such as suppliers, consultants, distributors, customers,

In other words, **anyone can be a whistleblower and MCG EMEA's reporting channels are open for everyone.**

II. Which violations can be reported by whistleblowers?

MCG EMEA provides protection for people who ask questions and/or report information, including reasonable suspicion, regarding actual or potential violations that have occurred or are very likely to occur, as well as attempts to conceal such violations.

The report may concern actual or potential breaches of mandatory laws, such as **EU law, national laws, internal policies and ethical violations.**

Some of topics that may be reported through MCG EMEA's whistleblower channels are:

- civil or criminal misconduct,
- Human rights,
- bribery, even among private parties
- breach of international treaties,
- public procurement,
- environmental protection,
- product safety and compliance,
- transport safety,
- nuclear safety,
- public health,

[1] EU Directive on the protection of persons who report breaches of Union law 2019/1937

- consumer protection,
- violations of EU competition rules,
- German Supply Chain Act[2] and similar legislation,
- financial services and combat money laundry
- infringements against corporate tax rules or directed at obtaining a tax advantage contrary to the object or purpose of the applicable corporate law,
- food safety, animal health and welfare,
- terrorist financing,
- Threat of prejudice to general interest
- infringements to the detriment of the EU's financial interests, and
- protection of privacy and personal data and security of network and information systems,
- In Italy, violation of "Modello 231".

III. What are MCG EMEA's reporting channels?

You can ***freely choose*** between:

- Safecall, a third-party platform in which reports can be made either orally or in written form, in your native language, either anonymously, semi anonymously (meaning that Safecall would know your identity, but will not disclose it to anyone in MCG EMEA) or on name basis, ***as you prefer***. In the corresponding list you will find the appropriate telephone number in your country,

- You can also make your report directly, even orally, to any member of MCG EMEA's Compliance Department. On the MCG EMEA's intranet site you will find the team members of MCG EMEA's Compliance Department, whom you can also contact directly, including in person,

- Contact directly your relevant management and/or local HR department,[3] and

- You can also send your report directly and confidentiality to MCG EMEA's Compliance Department at emea-ethics@mcgc.com.[3]

You will receive an acknowledgement of receipt within 7 days and a final assessment on follow-up measures taken and their justification after 3 months at the latest[4].

You may request to have physical or videoconference meetings within 20 working days.

In addition, you have the option of submitting your report to external reporting offices of the competent authorities.

IV. Are whistleblowers protected?

[2] *Lieferkettensorgfaltspflichtengesetz,* July 16th, 2021 (BGBl. I S. 2959)
[3] Based on Italian law this reporting channel is not applicable for MCG's affiliates in Italy. Please refer to other available reporting channels.
[4] In Slovakia, investigation feedback will be provided within 30 days pursuant with local laws.

Whistleblower‘s protection is guaranteed at MCG EMEA.

The identity of the whistleblower, as well any other information from which such identity may be identified directly or indirectly, shall not be disclosed, without the express written consent of the reporting party, to any person other than those who are expressly authorized to handle such report.

The MCG EMEA’s Compliance Department will ensure that the whistleblower is protected from any form of retaliation, such as:

- Termination,
- Denial of a promotion,
- Salary cut,
- Bullying,
- Discrimination,
- Harm on social media,
- Withdrawal of a license or permit,
- Negative performance appraisal, among others.

MCG EMEA’s Compliance Department also ensures protection against retaliation and protects the anonymity of any person that supports or collaborate with the investigation process conducted at MCG EMEA.

MCG EMEA’s Compliance Department will take the necessary steps to avoid conflict of interest while conducting investigations.

V. Speak up!

Take advantage of the opportunities to report violations to MCG EMEA’s Compliance Department. You will help ensuring that MCG EMEA complies with existing laws and regulations at all times, is a good employer and does not damage the group’s reputation.

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”), the UK General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (together the UK GDPR),as well as applicable national data protection regulations.As, the application of these laws depends on each individual case, 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 and UK GDPR

The processing of the reporting party's identification data is based on consent to be given (Art. 6 (1) lit. a GDPR and UK 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 and UK 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: Mitsubishi Chemical Europe GmbH, Schiessstraße 47, 40549 Düsseldorf

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 center 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 organizational 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 authorized.

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 authorized and specially trained employees of the MCG EMEA's Compliance Department of the responsible party and is always treated confidentially. The employees of the MCG EMEA's Compliance Department 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. If a recipient of your personal data is located in a country without adequate statutory data protection, we require and ensure the recipient to undertake to comply with data protection (for this purpose, we use the revised European Commission's standard contractual clauses, which can be accessed here) unless the recipient is subject to a legally accepted set of rules to ensure data protection. UK belongs to the countries outside of EU and EEA which ensure the same level of personal data protection as EU and EEA. For above mentioned reasons transfers to UK are permitted by European Commission in accordance with art. 45 of GDPR.

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 and UK 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 and UK GDPR.

Information of the accused person

In accordance with Art. 14 of the GDPR and UK 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.