Dokumententyp / Type of document	Konzernrichtlinie	**Vertraulichkeitsklasse / Confidentiality class**	1 Öffentlich
Titel / Title: VDM Whistleblower Guideline			
Dok.-Nr. / Doc.-No:	VDMS-0019816	**Revision / Revision:**	00
Bereich / Department	Compliance / / /		
Prozess / Process	Übergreifend / / / /		

Prüf und Genehmigungsverfahren / Review and Approval process

Ersteller / Author: Dania Hoffmann

Prüfer / Name reviewer:

Nicole Teresiak		

Freigabe / final approval	
Name / Name:	Matthias Moehle
Datum / date of approval:	19.06.2024

Inhaltsverzeichnis/Table of Content

1 Change History

Revision	Change	Reason of Change
00	Incorporation of requirements from ISO 37301-Standard	Incorporation of requirements from Whistleblower Protection Act (Hinweisgeberschutzgesetz - HinSchG)

Training information needed?: see VDMS

The new / changed text areas needs to be marked by the author in yellow colour.

1. Introduction

The VDM Metals Group is committed to a corporate culture based on good corporate governance and ethical behavior. This guideline implements the requirements of the ISO 37301, especially chapter 8.3, 8.4 and 10.2 and the German Whistleblower Protection Act (Hinweisgeberschutzgesetz - HinSchG).

2. Scope

This guideline applies to the entire VDM Metals Group and all of its subsidiaries, affiliates and joint ventures (collectively "VDM").

3. Aim and purpose

The aim of this guideline is to encourage employees and third parties to report unacceptable behavior within the company in order to prevent damage to the company.
Part of VDM's values and culture is that employees and third parties can report misconduct without fear of retaliation. VDM and its Management Board want to encourage behaviour that creates and supports compliance. Behaviour that is not compliant, on the other hand, is not tolerated and should be prevented through a speak up culture.
This guideline offers guidance in handling of violations, while respecting the rights of the individuals affected and data protection. Violation means all cases of noncompliance or nonconformity with any internal rules and regulations as well as respective laws, human rights and environmental due diligence obligations.
Any suspected violation should be reported as soon as possible. The aim of this guideline is to uncover criminal and other unlawful acts within the company that might otherwise remain hidden. The possibility of full anonymity ensures that employees are not at risk of any negative consequences for their employment relationship as a result of reporting.
The management is obligated to immediately check for indications of violations in order to be able to terminate and adequately prevent such violations if necessary. The overriding goal is to counteract violations in the company effectively and preventively.

4. Internal reporting process

4.1. General information

4.1.1. Persons authorized to report

The whistleblowing system is intended to enable reports on violations by both employees and third parties, such as suppliers and other business partners, affected persons or associations. VDM ensures that those persons are made aware of the available reporting channels, for example through regular communication.

4.1.2.Subjects of reports

The subject of a report may be, for example (not exhaustive):

- Offering or accepting bribes (corruption)
- Fraud
- Money laundering or misappropriation of funds
- Theft (especially above the de minimis threshold)
- Acts of violence

- Damage to property
- Tax offenses
- Violations of internal regulations and rules (confidentiality regulations, accounting regulations, etc.)
- Any violations of human rights and environmental due diligence obligations of the Act on Corporate Due Dilligence Obilgations in Supply Chains (Lieferkettensorgfaltspflichtengesetz - LkSG), including violations of the Code of Conduct for Suppliers by suppliers,
- Any other behavior that could have a detrimental effect on business or reputation

4.1.3. Internal and external reports

Whistleblowers have the option of submitting reports both internally and externally. In principle, an internal report should be preferred. Also, the whistleblower has the option of submitting an external report. For detailed information on external reporting offices, see point 7 of this guideline.

4.2. Basic principles

4.2.1. Confidentiality

The following information must be treated confidentially, also and especially during the performance of the comprehensive internal investigation:

- The identity of the whistleblower;
- The identity of the persons named in the report, including the person who is subject of the report;
- Any other information from which the identity of the whistleblower can be directly or individually inferred.

Any additional requirements under the respective national law must be observed.

4.2.2. Non-retaliation principle

It is a secondary obligation of the employee under the employment contract to inform the employer of all significant events in the company and, in particular, to prevent significant damage. This duty to prevent damage also obligates the employee to report impending damage and significant breaches of duty by other employees in the company. In this respect, the reporting of violations does not have any negative consequences for the whistleblower, in particular under labour law. This does not apply to the intentional disclosure of false information.
Whistleblowers are protected as far they provide information based on a good faith and belief that a violation has occurred. The motivation behind a whistleblower's action is irrelevant when assessing the validity of the allegations. Nevertheless, intentionally submitting a false report, whether oral or written, is deemed a violation itself and may result in disciplinary action.
Any whistleblower who feels threatened or feels that he has been retaliated against can provide a written complaint, describing the circumstances to the Chief Compliance Officer.
If whistleblowers themselves are involved in the compliance case, there is no general right to immunity from disciplinary, civil or labour law measures despite the non-retaliation approach. However, the fact that whistleblowers involved in the crime have contributed to the investigation must generally be taken into account in their favor when making a decision.

1.1.1.1

4.2.3. Data protection

The personal data of whistleblowers will be processed in accordance with the data protection information for the online reporting channel and in accordance with the provisions of the European General Data Protection Regulation (GDPR) and the national legal provisions, in particular the German Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG).

4.2.3.1. Collected and processed data

In the event of a report, the following personal data and information about the whistleblower will be collected and processed:

- the name or private contact and identification data, if the whistleblower voluntarily discloses his/her identity (non-anonymous report),
- the professional contact and (work) organization data, insofar as these are provided by the whistleblower (non-anonymous report).

In addition, the names of persons and other personal data of persons named by the whistleblower and relating to the reported facts may be collected and processed.

4.2.3.2. Purposes for the data processing

The personal data collected will be processed for the following purposes:

- Examination and processing of the report received and any associated investigations against the person(s) concerned by the report,
- Communication with authorities and courts in connection with the report,
- Communication with commissioned national and international law firms and auditing companies or investigators, such as detective agencies, and
- Communication with other companies of VDM, insofar as the reported facts do not concern only one company of VDM and the legal regulations for the protection of the identity of the whistleblower do not conflict with this.

4.2.3.3. Legal bases

The processing of personal data is based on the following legal bases:

- Processing of personal data relating to the whistleblower and the person(s) named in a report: Safeguarding the legitimate interests of the companies of VDM or a third party (Article 6 (1) sentence 1 lit. f) GDPR).
  It is a legitimate interest of the companies of VDM to act in accordance with the provisions of the Whistleblower Protection Act and to detect, process, remedy and sanction violations within the meaning of this guideline by employees throughout VDM, effectively and with a high degree of confidentiality, and to avert associated damage and liability risks for the companies.
- The legal basis for the processing of special categories of personal data is Art. 6 (1) sentence 1 lit. f) and Art. 9 (2) lit. g) GDPR in conjunction with Section 10 sentences 2 and 3 HinSchG.

4.2.3.4. Further information

Further information, for example on the transfer of personal data to authorities or other third parties, on the retention period and on the rights of employees as data subjects of the processing of their personal data can be found in the privacy guideline for the digital whistleblower system.

4.2.3.5. Involvement of the Data Protection Officer

Investigative measures involving the processing of personal data, in particular electronic data browsing, shall be agreed with the Data Protection Officer.

4.2.3.6. Involvement of third parties

Third parties involved in the processing of data must be obliged to comply with this obligations in order to achieve the greatest possible protection for the persons providing the information and related persons.

4.3. Procedure of internal reporting

4.3.1. Receipt and documentation of received reports

Possible violations can be reported through the following channels:

- Web-based VDM whistleblowing system, which can also be accessed anonymously via https://secure.ethicspoint.eu/domain/media/de/gui/105118/index.html1
- E-mail to the VDM Compliance Department via compliance@vdm-metals.com or compliance.vdm@vdm-metals.com
- Use of the internal compliance hotline at extension -7777 (from outside the company: +49 2392 55 7777)
- Personal notification to the Chief Compliance Officer, the Compliance Officers, managers or employees in supervisory roles.

The Compliance Officers, managers and employees in supervisory roles who receive a report alleging suspected violation shall ensure that the matter is promptly reported to the Chief Compliance Officer.
The Chief Compliance Officer conducts an initial relevance test to see if the reported case is relevant for the Compliance Management System.
The Chief Compliance Officer then informs the Compliance Committee and the Group Compliance Officer (= Chief Compliance Officer of Acerinox S.A.) of any compliance relevant report received.
The Compliance Committee consists in any case of the following persons at VDM and manages the review of these indications:

- General Counsel,
- Chief Compliance Officer,
- Head of Internal Audit.

In addition, the Chief Compliance Officer decides on a case-by-case whether other functions such as CEO or the Head of HR or another executive function should become part of the Compliance Committee. The Chief Compliance Officer ensures that the report and the information regarding the report is documented in writing and carefully examined using one of the above reporting channels.
At the latest within seven days of receipt of his report, the whistleblower will receive feedback that his report has been received.

4.4. Evaluation process and evaluation criteria

4.4.1. Plausibility check

If possible, an interview is first held with the whistleblower (anonymously if desired). Afterwards, the report and all information contained therein must be checked for possible violations and its plausibility.

If the reported abnormalities are based on a concretely identifiable key fact, if it is possible and not improbable that a legal or regulatory violation has occurred in the corporate sphere, and if the possible violation is relevant from a compliance point of view, the facts must be clarified further in an internal investigation.
The following information must be treated confidentially during the plausibility check:

- The identity of the whistleblower;
- The identity of the persons named in the report, including the subject of the report;
- Any other information from which the identity of the whistleblower can be inferred directly or indirectly.

Any additional requirements under applicable national law must be observed.

4.4.2. Voting on further steps

The Compliance Committee shall consider, taking into account the circumstances of the individual case and the applicable legal provisions, whether it is necessary to conduct an internal investigation to clarify the information or whether the information received should not be pursued further.
In the event of a tie vote regarding the decision, the Chief Compliance Officer has the deciding vote. If a member of the Compliance Committee is subject of the report it should not be involved in the decision.
The Compliance Committee shall determine at its own discretion whether the involvement of other specialist departments is necessary for decision-making.
The more relevant the reported legal violation is, the greater the obligation to initiate an internal investigation. For this purpose, the following criteria, among others, must be taken into account:

- Initial suspicion of a criminal act (sufficient factual evidence),
- Severity of the reported violation,
- Number and duration of violations,
- Risk of major financial loss,
- Large number of potentially injured parties,
- Existence of comparable legal violations in the past (whether known to the authorities or not),
- Indications of a systematic approach,
- Threat of fines, penalties and damages,
- The likelihood that the violation may be defamatory,
- Knowledge of law enforcement or other authorities or a high risk of detection.

A subsequent, comprehensive internal investigation of a report can be waived, if the prior plausibility check shows that the suspicion is not based on any actual facts, can be eliminated by simple means or is only a minor violation.
If clarification measures are waived, this must be carefully documented and justified, and the whistleblower must be informed accordingly.
In order to safeguard legal claims, it must be examined whether and in what form (if necessary, while preserving anonymity) a report should be made to insurers.
It must also consider whether to involve regulatory or judicial authorities. In case it is required by law to inform the authorities about violations, the respective authorities shall be informed in accordance with the applicable regulations, or as otherwise agreed.
Even in case it is not required by law to report violations, a voluntary self-disclosure of the violation to authorities to mitigate the consequences of the violation can be considered.
The decision in this regard is made within 14 days of receipt of a report. The whistleblower must be informed accordingly.
If the whistleblower wishes to remain anonymous, his or her identity and all other information concerning him or her may only be disclosed if this is absolutely necessary to fulfill a legal obligation in the context of official or judicial investigations.

4.4.3. Ad-hoc reporting

In the event of serious suspected violations, the Chief Compliance Officer shall inform the CEO.
A serious suspected violation is deemed to exist if, following a plausibility check, serious financial damage or serious damage to the company's reputation has occurred or threatens to occur.
Ad-hoc reporting is not required if, upon careful consideration and weighing of the specific violation's circumstances, the Compliance Committee determines that the occurrence of the loss is uncertain, unlikely or only slight. The decision and its reasons shall be documented.

5. Internal investigation process

5.1. Investigation team and procedure

If an internal investigation is initiated, the Compliance Committee must decide which department or persons are responsible for the further clarification of a received report, which procedures (such as personal interviews, data analyses, collection of information from external sources, etc.) must be carried out and whether external experts such as auditors, IT forensic experts and lawyers must be consulted. In the event of a tie vote regarding the decision, the Chief Compliance Officer has the deciding vote.
VDM ensures that all investigations held according to reported violations are fair and independent.

5.2. Conflicts of interest

For the internal investigation, the principle of independence applies and thus, in particular, the "prohibition of self-control": persons whose possible violation is being investigated may neither lead, be responsible for, nor operatively conduct the investigation.

5.3. Involvement of works council

Before an investigation is carried out, the Chairman of the competent Works Council must be informed if a measure falls within the works council's area of responsibility.

5.4. Process flow

The following procedural steps are performed when conducting the internal investigation:

- Determination of the scope of the investigation
- Determination of the responsibilities of the persons involved
- Examination of a "litigation hold" and data backups while maintaining the protection of personal data
- Identification and investigation of the reported violation
- Collection and sifting of evidence in compliance with the regulations for securing and evaluating evidence
- Isolation of suspicious persons, if necessary
- Possibly after clarification with the insurance company: commissioning of additional legal support (by external lawyers) and/or technical support (by external experts or forensic specialists), if necessary
- Ensuring the traceability of conclusions and results
- Quality control

The Chief Compliance Officer is responsible for taking immediate measures to immediately stop the compliance breach.

5.4.1. Access to documents and data

Official documents in paper form may be inspected by the investigation team or by the third parties commissioned with the investigation within the framework of the applicable legal provisions and in compliance with the protection of personal data. Special protection of private documents (e.g., secrecy of correspondence) must be observed.
Before inspecting computers and data (especially employees' e-mail inboxes), special attention must be paid to data protection regulations.
Employees' e-mail inboxes may only be viewed with prior consent and/or within the limits of applicable national law.
If data is processed neither to clarify a criminal offense nor for the purpose of the employment relationship (e.g. data processing by third parties), it must be checked whether standards on consent apply in the individual case.
Any access must comply with the principle of proportionality and all measures must be defined in such a way that any impairment of the legitimate interests of the person concerned is mitigated as far as possible (e.g. limitation of the time period, clear search criteria, need-to-know basis, immediate sorting out of recognizably private e-mails).
Files that are recognizably private may not be accessed.

5.4.2. Visual inspections of the offices

Based on the employer's domiciliary rights, an employee's office may be visually inspected without the employee's knowledge or consent if an investigation so requires. Any deviating legal regulations at the place of the visual inspection must be observed.

5.4.3. Interview of employees, former employees and third parties

Employees who are interviewed as part of the internal investigation are generally obligated as part of their employment relationship (among other things, due to the duty of loyalty under their employment contract) to

- participate in the survey,
- communicate with the employer and
- provide truthful information within the contractually defined scope of duties.

At the beginning of the interview, the background of the investigation, the suspicions and the possible recipients of the information provided by the interviewee must be made clear.
It is necessary to check whether further instructions and information are required under national law (e.g. the right to refuse to provide information, the possibility of involving third parties, data protection requirements).
The aforementioned principles also apply mutatis mutandis to former employees and to third parties, although the obligation to disclose information may be limited.
The statements of the employees must be documented word for word as far as possible without being subjectively interpreted by the person recording them. The interviewed person must have the opportunity to review the transcript, correct it if necessary and confirm it with his or her signature.

5.4.4. Chance finds

If a "chance find" is made during the investigation that provides indications of a legal or regulatory violation based on a substantially and completely different set of facts, a new, separate investigation must be initiated. In such a case, the admissibility of this new investigation and the obligations to provide instructions and information (such as the right to refuse information, the possibility of calling in third parties and the requirements under data protection law) must be re-examined.

5.5. Conclusion after completion of the investigation

5.5.1. Responsibility and final report

The Compliance Committee decides on the consequences of any violation identified, which may include notifying the relevant authorities or imposing sanctions depending on the severity of the violation.
The approval of three of the four members of the Compliance Committee is sufficient to close an investigation.
Completion of the investigation requires the Chief Compliance Officer to prepare a final report that must include, at a minimum, the following:

- Presentation of the results and objective response to the reported violation,
- Summary of the facts,
- Description of the information and documents on which the investigation is based,
- Explanation of the results,
- Conclusions, consequences, remedial actions and proposals resulting from the investigation,
- Description of identified roots that caused a violation, vulnerabilities of the compliance management system and accountability lapses, including among managers, top management and the governing body.
- Recommendations concerning a potential review or update of the Compliance Management System

5.5.2. Decisions on sanctioning

The final decision to impose sanctions shall be made by the Compliance Committee on the basis of the investigation report, taking into account the circumstances of the individual case, the seriousness of the violation, the position of the acting persons in the company and the requirements of labour and corporate law.
In the event of a tie vote regarding the decision, the Chief Compliance Officer has the deciding vote. If a member if the Compliance Committee is subject of the report it should not be involved in the decision. Where necessary, the relevant works council shall be involved.
If the violation results in disciplinary action under employment law, this shall be carried out by HR and, if necessary, by the relevant competent body.
Where appropriate, the person concerned shall be given the opportunity to comment. The employment action shall be documented in the personnel file via HR.
The provisions of labour and works constitution law shall remain unaffected.

5.5.3. Return of evidence and deletion of data

Evidence must be returned after the investigation is completed.
If the purposes for which personal data were collected or otherwise processed no longer apply, in particular if they are not required for the assertion, exercise or defense of legal claims, they must be deleted or anonymized after the investigation has been completed.

5.6. Notification of the whistleblower

The Chief Compliance Officer will send the whistleblower an interim report on the status of the investigation no later than three months after receiving the report. After completion of the investigation, the whistleblower will receive a final message. The messages must contain information on confidentiality and on how to reach the whistleblower for further inquiries.

5.7. Reporting obligations

5.7.1. Reporting to the Group Chief Compliance Officer

The Chief Compliance Officer shall inform the Group Chief Compliance Officer immediately of each report received and successively of each subsequent investigation step and its outcome. The Group Chief Compliance Officer shall inform the VDM Audit Committee accordingly at its next regular meeting.
Communication to the Group Chief Compliance Officer is anonymized and always takes into account data protection regulations.

5.7.2. Regular reporting to the Executive Board and the Supervisory Board

The Chief Compliance Officer shall prepare an overview of the reports received during the *[quarterly]* reporting and their status, which is presented to the Executive Board and the Supervisory Board at their regular meetings, conducted *[quarterly]* or in the event of serious suspected violations ad hoc.
Information about reports received, the status and results of the internal investigation and the consequences are considered in the Management Review according to Chapter 9.3 of ISO 37301.

5.8. Documentation and archiving

The Chief Compliance Officer keeps a register of all reports received. The date of receipt, the course of the investigation and the measures taken must be documented in this register.
Documentation of reports that prove to be unfounded after internal investigation is kept in accordance with the statutory retention periods; documentation of reports that result in the notification of the competent authorities or the imposition of sanctions or further consequences (civil or labour) is also kept in accordance with the statutory retention periods, in compliance with national data protection regulations.

6. Nonconformity and corrective action process

6.1. Response trough controlling, correction and consequence management

In case a violation occurs, an immediate reaction should follow and if applicable:

- the actions to control and correct it shall be taken promptly,
- the consequences arising from the identified violation shall be respectively addressed and managed.

6.2. Assessment of the causes of violations

A thorough root-cause analysis addresses the extent and pervasiveness of the violation, the number and level of the personnel involved, and the seriousness, duration and frequency of the violation. The necessity for taking further actions to address the root cause(s) of the violation should be assessed and evaluated to prevent recurrence or occurrence.
This evaluation should involve a revision of the violation, a determination of the causes of the violation and a determination if similar violations exist, or can potentially occur in the future.

6.3. Implementation of measures

In pursuit of the commitment to quality and compliance, VDM underscores the significance of implementing measures to address identified violations. This involves the implementation of any actions required, a thorough evaluation of the effectiveness of taken corrective measures, and potential adjustments to the compliance management system, if deemed necessary.
Corrective actions shall be appropriate to the effects of the violations.
Documented information shall be available as evidence of:

- the nature of identified violations,
- the subsequent actions taken in response to these cases,
- the results achieved through the implementation of corrective actions.

By adhering to this clause, VDM remains dedicated to continuous improvement, ensuring the highest standards of quality and compliance in all facets of company operations.

6.4. Improvement of the Compliance Management System

In the event that compliance violations are detected during the internal investigation, the Compliance Committee will decide on the necessity a potential review or update of the Compliance Management System, where applicable. Insights gained during internal investigations are used to evaluate the performance of the Compliance Management System, where appropriate.
When planning the Compliance Management System according to ISO 37301 Chapter 6, the findings of the internal investigations are taken into consideration. Planning in this context means to anticipate potential scenarios and consequences and it is, as such, preventive. Based on the findings of the internal investigations, the organization should plan how to address undesired effects before they occur and how to benefit from favourable conditions or circumstances that can support the effectiveness of the Compliance Management System.
Also, lessons learned from the reports and the internal investigations can be used as examples in trainings for the employees taking into account the requirements of data protection law.
The compliance risks are reassessed by the Chief Compliance Officer whenever there are violations(s) and/or near-misses.

6.5. Documentation

The Chief Compliance Officer will keep documented information about all relevant information of the investigation, in particular regarding the nature of the compliance violation and the measures taken.

7. External reporting

Whistleblowers can also contact the external reporting offices at any time. The reporting channels of the federal government's external reporting offices are listed below.

7.1. Federal Office of Justice

The Federal Office of Justice is generally responsible for external reports. Reports can be submitted anonymously. Possible violations can be reported trough the following channels:

- Online via
- https://formulare.bfj.bund.de/ffw/form/display.do?%24context=F3ADF865168B225E841D
- By mail to:
  Bundesamt für Justiz
  Externe Meldestelle des Bundes
  53094 Bonn

- By phone via number +49 228 99 410-6644
- Personally (by appointment) at:
  Bundesamt für Justiz
  Externe Meldestelle des Bundes
  53094 Bonn

7.2. Federal Financial Supervisory Authority

The Federal Financial Supervisory Authority (BaFin) is responsible for reports in connection with violations that it is responsible for prosecuting and punishing in accordance with Section 4d FinDAG. Reports can be submitted anonymously. Possible violations can be reported trough the following channels:

- Online via
  https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=2BaF6&c=-1&language=ger
- By mail to:
  Bundesanstalt für Finanzdienstleistungsaufsicht
  Hinweisgeberstelle
  Graurheindorfer Straße 108
  53117 Bonn
- By phone via number +49 228 4108 – 2355
- Personally at:
  Bundesanstalt für Finanzdienstleistungsaufsicht
  Hinweisgeberstelle
  Dreizehnmorgenweg 44-48
  53175 Bonn

7.3. Federal Cartel Office

The Federal Cartel Office is responsible for special antitrust cases (cartels, market abuse). Reports can be submitted anonymously. Possible violations can be reported trough the following channels:

- Online via
- https://www.bkms-system.net/bkwebanon/report/channels?id=bkarta&language=ger
- By mail to:
  Bundeskartellamt
  Externe Meldestelle
  Kaiser-Friedrich-Straße 16
  53113 Bonn
- By phone via number +49 228 9499 - 5980
- Personally at:
  Bundeskartellamt
  Externe Meldestelle
  Kaiser-Friedrich-Straße 16
  53113 Bonn

8. General responsibility

The responsibility of this guideline lies with:
Author: Nicole Teresiak, CCO/Head of Compliance
Reviewer: Matthias Möhle, General Counsel
Releaser: Dr. Niclas Müller, Chairman of the Management Board

9. Review and adaption

The guideline is regularly checked to ensure that it is up to date and amended if necessary. If the need for changes or additions is identified outside the regular review, the guideline will be amended accordingly on an ad-hoc basis.