

Dokumententyp:	Richtlinie	Vertraulichkeits- klasse:	2 intern
Titel / Title: VDM Richtlinie - Interne Untersuchungen			
Dok.-Nr.:	908108-004	Revision:	00
Bereich:	Recht		
Ersteller: (Name/Datum):	Nicole Teresiak, 03.07.2023		
Freigabe (Name/Datum):	Prüfer: Matthias Möhle, 06.07.2023 Freigeber: Dr. Niclas Müller, 06.07.2023		

1. Änderungshistorie:

Revision	Änderung	Änderungsgrund
00	Erstellung	Neuerstellung

2. Geltungsbereich

Diese Richtlinie gilt für die gesamte VDM Metals Group sowie alle ihre Tochtergesellschaften, verbundene Unternehmen und Gemeinschaftsunternehmen (gemeinsam "VDM").

3. Ziel und Zweck

Ziel und Zweck dieser Richtlinie ist, die Gewährleistung eines angemessenen, standardisierten Umgangs mit eingegangenen Hinweisen. In dieser Richtlinie werden die Grundsätze der Bearbeitung verbindlich definiert, um einen einheitlichen Maßstab für die Einleitung, Durchführung und Dokumentation interner Prüfungen infolge eingegangener Hinweise sicherzustellen.

Zur Bearbeitung hinzugezogene Dritte sind zur Einhaltung entsprechend zu verpflichten, um einen größtmöglichen Schutz hinweisgebender Personen sowie damit im Zusammenhang stehender Personen zu erreichen.

Die Geschäftsleitung ist zur unverzüglichen Prüfung von Hinweisen auf Verstöße gegen interne Regeln oder Gesetze im Unternehmen verpflichtet, um solche ggf. abstellen und adäquat ahnden zu können. Übergeordnetes Ziel ist es, Rechts- und Regelverstöße im Unternehmen effektiv und präventiv entgegenzuwirken.

4. Zuständigkeiten

Der Chief Compliance Officer informiert das Compliance Committee über eingegangene Hinweise. Das Compliance Committee besteht aus folgenden Personen der VDM und steuert die Prüfung dieser Hinweise:

- CEO
- General Counsel
- Chief Compliance Officer
- Leiter Interne Revision

5. Verfahren

5.1 Entgegennahme und Dokumentation eingegangener Hinweise

Ein mögliches Fehlverhalten in Form von Rechts- oder Regelverstößen kann über folgende Kanäle gemeldet werden:

- Webbasiertes VDM-Hinweisgebersystem, welches auch anonym erreichbar ist via

<https://secure.ethicspoint.eu/domain/media/de/gui/105118/index.html>¹

- E-Mail an die VDM-Compliance-Abteilung via compliance@vdm-metals.com
- Nutzung der internen Compliance-Hotline unter der Durchwahl -7777 (von außerhalb des Unternehmens: +49 2392 55 7777)
- Persönliche Hinweiserteilung an den Chief Compliance Officer

Der Chief Compliance Officer stellt sicher, dass Hinweise unter Nutzung einer der vorstehenden Meldewege dokumentiert und sorgfältig geprüft werden. Im Rahmen eines regelmäßigen Austauschs mit den Mitgliedern des Compliance Committees wird einzelfallbezogen festgelegt, ob und ggf. wie ein eingegangener Hinweis konkret weiterverfolgt werden soll.

Spätestens innerhalb von sieben Tagen nach Eingang seines Hinweises erhält der Hinweisgeber die Rückmeldung, dass sein Hinweis eingegangen ist und untersucht wird.

5.2 Abstimmung über weitere Prüfschritte

Das Compliance Committee prüft unter Berücksichtigung der Umstände des Einzelfalls und der geltenden Rechtsvorschriften, ob die Durchführung einer internen Prüfung zur Aufklärung des Hinweises geboten ist oder ob der erhaltene Hinweis nicht weiterverfolgt wird. Das Compliance Committee bestimmt nach eigenem Ermessen, ob die Hinzuziehung anderer Fachabteilungen zur Entscheidungsfindung erforderlich ist.

Es muss auch prüfen, ob Verwaltungs- oder Justizbehörden einzuschalten sind. Die diesbezügliche Entscheidung wird innerhalb von 14 Tagen nach Eingang eines Hinweises getroffen. Der Hinweisgeber muss entsprechend informiert werden.

6. Bewertungsprozess und Bewertungskriterien

6.1 Plausibilitätsprüfung

Zunächst findet nach Möglichkeit ein Gespräch mit dem Hinweisgeber statt (auf Wunsch auch anonym). Danach müssen Hinweise bzw. Sämtliche darin enthaltene Informationen auf ein mögliches Fehlverhalten und dessen Plausibilität geprüft werden.

Beruhend auf den gemeldeten Auffälligkeiten auf einem konkret erkennbaren Schlüsselbestand, ist es möglich und nicht unwahrscheinlich, dass ein Rechtsverstoß in der Unternehmenssphäre begangen wurde, und ist der mögliche Rechtsverstoß unter Compliance-Gesichtspunkten relevant, muss der Sachverhalt weiter aufgeklärt werden.

Zur Wahrung von Rechtsansprüchen ist zu prüfen, ob und in welcher Form (ggf. unter Wahrung der Anonymität) eine Meldung an Versicherer erfolgen sollte.

Auf eine sich anschließende, umfassende interne Prüfung eines Hinweises kann verzichtet wer-

¹ Des Weiteren steht Hinweisgebern das Acerinox-Hinweisgebersystem zur Nutzung zur Verfügung. Das Verfahren der Bearbeitung dort eingegangener Hinweise ist in einer separaten Prozessbeschreibung festgeschrieben, welche u.a. unter folgendem Link abrufbar ist: https://www.vdm-metals.com/fileadmin/user_upload/Unser_Unternehmen/02_Ueber_VDM_Metals/02_05_Unternehmerische_VW/02_05_d_Code_of_Conduct/Acerinox_Procedure_for_reports.pdf.

den, wenn die vorherige Plausibilitätsprüfung ergibt, dass dem Verdacht keine tatsächlichen Anhaltspunkte zugrunde liegen, er mit einfachen Mitteln ausgeräumt werden kann oder es sich nur um einen Bagatelldelikt handelt. Die folgenden Informationen müssen während der Plausibilitätsprüfung vertraulich behandelt werden:

- Die Identität des Hinweisgebers
- Die Identität der in dem Bericht genannten Personen
- Alle anderen Informationen, aus denen die Identität des Hinweisgebers direkt oder indirekt abgeleitet werden können

Darüber hinaus gehende Anforderungen nach anwendbarem nationalen Recht sind zu beachten. Wünscht der Hinweisgeber anonym zu bleiben, dürfen seine Identität und alle anderen genannten Informationen die ihn betreffen, nur dann offengelegt werden, wenn dies zur Erfüllung einer Rechtspflicht im Rahmen von behördlichen oder gerichtlichen Ermittlungen zwingend erforderlich ist.

Je relevanter der gemeldete Rechtsverstoß ist, desto größer ist die Pflicht, eine interne Untersuchung einzuleiten. Zu diesem Zweck sind unter anderem folgende Kriterien zu berücksichtigen:

- Anfangsverdacht einer kriminellen Handlung (hinreichend tatsächliche Beweise),
- Schwere des gemeldeten Verstoßes,
- Anzahl und Dauer der Rechtsverstöße,
- Gefahr eines großen finanziellen Verlustes,
- große Anzahl potenziell Geschädigter,
- Vorhandensein vergleichbarer Rechtsverstöße in der Vergangenheit (unabhängig davon, ob sie den Behörden bekannt sind oder nicht),
- Hinweise auf ein systematisches Vorgehen,
- Androhung von Geldstrafen, Bußgeldern und Schadensersatz,
- die Wahrscheinlichkeit, dass das Fehlverhalten verleumderisch sein könnte,
- Kenntnis der Strafverfolgungsbehörde oder anderer Behörden oder ein hohes Risiko der Entdeckung.

Wird auf Aufklärungsmaßnahmen verzichtet, ist dies sorgfältig zu dokumentieren und zu begründen und der Hinweisgeber entsprechend darüber zu informieren.

6.2 Durchführung einer umfassenden, internen Prüfung

6.2.1 Prüfungsteam und Verfahren

Wird eine interne Prüfung eingeleitet, muss das Compliance Committee entscheiden, welche Fachabteilung oder Personen für die weitere Aufklärung eines eingegangenen Hinweises jeweils zuständig sind, welche Verfahren (wie persönliche Befragungen, Datenanalysen, Einholung von Informationen aus externen Quellen usw.) durchgeführt werden müssen und ob externe Experten wie Wirtschaftsprüfer, IT-Forensiker und Anwälte hinzugezogen werden müssen.

6.2.2 Prozessablauf

Die folgenden Verfahrensschritte werden bei der Durchführung der internen Untersuchung durchgeführt:

- Festlegung des Umfangs der Untersuchung
- Festlegung der Verantwortlichkeiten der beteiligten Personen
- Prüfung eines "Litigation Hold" und von Datensicherungen unter Wahrung des Schutzes personenbezogener Daten
- Identifizierung und Untersuchung des gemeldeten Fehlverhaltens
- Sammlung und Sichtung von Beweismitteln unter Beachtung der Vorschriften zur Beweissicherung und -auswertung
- Isolierung verdächtiger Personen, falls erforderlich
- Eventuell nach einer Klärung mit der Versicherung: Beauftragung von zusätzlicher rechtlicher Unterstützung (durch externe Anwälte) und/oder technischer Unterstützung (durch externe Experten oder Forensiker), falls erforderlich
- Sicherstellung der Nachvollziehbarkeit der Schlussfolgerungen und Ergebnisse
- Qualitätskontrolle

6.2.3 Vertraulichkeit

Die folgenden Informationen müssen auch und gerade während der Durchführung der umfassenden, internen Prüfung vertraulich behandelt werden:

- Die Identität des Hinweisgebers
- Die Identität der in dem Bericht genannten Personen
- Alle anderen Informationen, aus denen die Identität des Hinweisgebers direkt oder indirekt abgeleitet werden kann

Darüber hinaus gehende Anforderungen nach dem jeweiligen nationalen Recht sind zu beachten.

6.2.4 Zugang zu Dokumenten und Daten

Offizielle Dokumente in Papierform können von Vorgesetzten oder Kollegen eines Mitarbeiters oder von den mit der Untersuchung beauftragten Dritten im Rahmen der geltenden Rechtsnormen und unter Wahrung des Schutzes personenbezogener Daten eingesehen werden. Ein besonderer Schutz privater Dokumente (z. B. das Briefgeheimnis) ist zu beachten.

Vor der Einsichtnahme in Computer und Daten (insbesondere in die E-Mail-Postfächer der Mitarbeiter) müssen die Datenschutzbestimmungen besonders beachtet werden.

Die E-Mail-Postfächer der Mitarbeiter dürfen nur mit vorheriger Zustimmung und/oder innerhalb der Grenzen des geltenden nationalen Rechts eingesehen werden.

Werden Daten weder zur Aufklärung einer Straftat noch zum Zweck des Beschäftigungsverhältnisses verarbeitet (z.B. Datenverarbeitung durch Dritte), ist zu prüfen, ob im Einzelfall Normen zur Einwilligung gelten.

Ein eventuell bestellter Datenschutzbeauftragter muss vor dem Zugriff hinzugezogen werden.

Jeder Zugriff muss dem Grundsatz der Verhältnismäßigkeit genügen und alle Maßnahmen

müssen so definiert sein, dass eine Beeinträchtigung der berechtigten Interessen der betroffenen Person so weit wie möglich abgemildert wird (z. B. Begrenzung des Zeitraums, klare Suchkriterien, Need-to-know-Basis, sofortiges Aussortieren erkennbar privater E-Mails).

Auf Dateien, die erkennbar privat sind, darf nicht zugegriffen werden.

6.2.5 Visuelle Inspektionen der Büros

Aufgrund des Hausrechts des Arbeitgebers kann das Büro eines Arbeitnehmers auch ohne dessen Wissen oder Zustimmung einer Sichtkontrolle unterzogen werden, wenn eine Untersuchung dies erfordert. Etwaige abweichende gesetzliche Regelungen am Ort der Sichtkontrolle sind zu beachten.

6.2.6 Befragung von Mitarbeitern, ehemaligen Mitarbeitern und Dritten

Arbeitnehmer, die im Rahmen der Untersuchung befragt werden, sind in der Regel im Rahmen ihres Arbeitsverhältnisses verpflichtet (u.a. aufgrund der arbeitsvertraglichen Loyalitätspflicht)

- sich an der Befragung zu beteiligen,
- mit dem Arbeitgeber zu kommunizieren und
- im Rahmen des vertraglich festgelegten Aufgabenbereichs wahrheitsgemäße Angaben zu machen. Bei der Befragung müssen zu Beginn der Hintergrund der Untersuchung, die Verdachtsmomente und die möglichen Empfänger der von der befragten Person übermittelten Informationen klargestellt werden.
- Es ist zu prüfen, ob weitere Anweisungen und Informationen nach nationalem Recht erforderlich sind (z. B. das Recht, die Auskunft zu verweigern, die Möglichkeit, Dritte hinzuzuziehen, Datenschutzanforderungen).

Die vorgenannten Grundsätze gelten sinngemäß auch für ehemalige Mitarbeiter und für Dritte, wobei allerdings die Verpflichtung zur Weitergabe von Informationen eingeschränkt werden kann.

Die Aussagen der Mitarbeiter müssen so weit wie möglich Wort für Wort dokumentiert werden, ohne dass sie von der aufzeichnenden Person subjektiv interpretiert werden. Der Hinweisgeber muss die Möglichkeit haben, die Niederschrift zu prüfen, sie gegebenenfalls zu korrigieren und mit seiner Unterschrift zu bestätigen.

6.2.7 Zufallsfunde

Wird während der Untersuchung ein "Zufallsfund" gemacht, der Hinweise auf ein Fehlverhalten gibt, das auf einem wesentlich und völlig anderen Sachverhalt beruht, so muss ein neues, gesondertes Aufklärungsverfahren eingeleitet werden. In einem solchen Fall ist die Zulässigkeit dieser neuen Untersuchung und die Weisungs- und Informationspflichten (wie z.B. das Auskunftsverweigerungsrecht, die Möglichkeit, Dritte hinzuzuziehen, und die datenschutzrechtlichen Anforderungen) neu zu prüfen.

6.2.8 Interessenkonflikte

Für die interne Untersuchung gilt der Grundsatz der internen Aufklärung auf der Grundlage unabhängiger Maßnahmen und damit insbesondere das "Verbot der Selbstkontrolle": Personen, deren Verhalten untersucht wird, dürfen die Untersuchung weder leiten, verantworten noch operativ durchführen.

6.3 Schlussfolgerung nach Prüfungsabschluss

6.3.1 Zuständigkeit und Abschlussbericht

Das Compliance Committee entscheidet über die Konsequenzen eines festgestellten Fehlverhaltens, zu denen je nach Schwere des Fehlverhaltens die Benachrichtigung der zuständigen Behörden oder die Verhängung von Sanktionen gehören kann. Das VDM Compliance-Management-System muss möglicherweise angepasst oder korrigiert werden, um ähnliche Rechtsverstöße in Zukunft zu verhindern.

Die Zustimmung dreier der vier Mitglieder des Compliance Committees genügt, um einen Prüfungsfall abzuschließen. Die Entscheidung, den Fall den zuständigen Behörden zu melden oder Sanktionen zu verhängen, trifft jedoch der CEO.

Der Abschluss der Prüfung verlangt die Erstellung eines Abschlussberichts durch den Chief Compliance Officer, der Folgendes mindestens enthalten muss:

- Präsentation der Ergebnisse und objektive Reaktion auf das gemeldete Fehlverhalten
- Zusammenfassung des Sachverhalts
- Beschreibung der Informationen, auf die sich die Untersuchung stützt
- Beschreibung der angewandten Ermittlungsmethoden und -techniken
- Erläuterung der Art und Weise, in der die Beweise erhoben wurden
- Erläuterung der Ergebnisse
- Schlussfolgerungen, Konsequenzen, Abhilfemaßnahmen und Vorschläge, die sich aus der Untersuchung ergeben

6.3.2 Rückgabe von Beweismittel und Löschen von Daten

Beweismittel müssen nach Abschluss der Ermittlungen zurückgegeben werden.

Wenn die Zwecke, für die personenbezogene Daten erhoben oder anderweitig verarbeitet wurden, nicht mehr gelten, insbesondere wenn sie nicht zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden, müssen sie nach Abschluss der Untersuchung gelöscht oder anonymisiert werden.

6.3.3 Benachrichtigung des Hinweisgebers

Der Chief Compliance Officer wird dem Hinweisgeber spätestens drei Monate nach Hinweiseingang einen Zwischenbericht über den Stand der Ermittlungen schicken. Nach Abschluss der Untersuchung erhält der Hinweisgeber eine Abschlussmitteilung. Die Nachrichten müssen Informationen über die Vertraulichkeit und die Erreichbarkeit für Nachfragen enthalten.

6.3.4 Schutz des Hinweisgebers

Es ist eine arbeitsvertragliche Nebenpflicht des Arbeitnehmers, den Arbeitgeber über alle wesentlichen Vorgänge im Betrieb zu unterrichten und insbesondere erhebliche Schäden abzuwenden. Diese Schadensverhütungspflicht verpflichtet den Arbeitnehmer auch zur Anzeige drohender Schäden und erheblicher Pflichtverletzungen durch andere Mitarbeiter im Unternehmen. Insofern hat die Meldung eines Fehlverhaltens keine negativen - insbesondere arbeitsrechtlichen - Konsequenzen für den Hinweisgeber. Dies gilt nicht für die vorsätzliche Weitergabe von Falschinformationen.

6.3.5 Kommunikation an den Group Chief Compliance Officer

Der Chief Compliance Officer informiert den Group Chief Compliance Officer aus dem Hause der Acerinox-Gruppe unverzüglich über jeden eingegangenen Hinweis und sukzessive über jeweils sich anschließende Prüfungsschritte und deren Ergebnis. Der Group Compliance Officer informiert das Audit Committee der Acerinox S.A. im Rahmen seiner nächsten regelmäßigen Sitzung entsprechend.

Die Kommunikation an den Group Chief Compliance Officer erfolgt regelmäßig anonymisiert und stets unter Berücksichtigung datenschutzrechtlicher Bestimmungen.

7. Dokumentation und Archivierung

Das Compliance Committee erstellt jährlich einen Bericht über seine Tätigkeit. Dieser Bericht muss die Anzahl und die Art der eingegangenen Meldungen, ihren Ursprung (intern oder extern), die Anzahl der durchgeführten Prüfungen, die daraus gezogenen Schlussfolgerungen, ihre Folgen und die getroffenen Korrektur-/Präventionsmaßnahmen enthalten.

Der Chief Compliance Officer führt ein Register mit allen eingegangenen Hinweisen. Das Eingangsdatum, der Verlauf der Untersuchung und die getroffenen Maßnahmen müssen in diesem Register dokumentiert werden.

Die Dokumentation von Hinweisen, die sich nach ihrer Untersuchung als unbegründet erweisen, wird mindestens ein Jahr lang aufbewahrt; die Dokumentation von Hinweisen, die zur Benachrichtigung der zuständigen Behörden oder zur Verhängung von Sanktionen oder weiteren Konsequenzen (zivil- oder arbeitsrechtlicher Art) führen, wird unter Beachtung der nationalen Datenschutzbestimmungen mindestens fünf Jahre lang nach Abschluss des Falles aufbewahrt. Weitere Aufbewahrungspflichten bleiben davon unberührt.

8. Verantwortlichkeit

Die Verantwortung dieser Richtlinie liegt bei:

Autorin: Nicole Teresiak, CCO/Head of Compliance

Prüfer: Matthias Möhle, General Counsel

Freigeber: Dr. Niclas Müller, Vorsitzender der Geschäftsführung