



WHITEPAPER: WHISTLEBLOWER-RICHTLINIE UND COMPLIANCE MANAGEMENT

Pflicht und Chance für Unternehmen

Nürnberg, Februar 2022

Karin Scherer
karin.scherer@scherer-concept.de

Inhaltsverzeichnis

1	<i>Überblick</i>	2
2	<i>Vorbemerkungen zum Hinweisgeberschutz – Gesetz-</i>	3
2.1	Worum geht es?	3
2.2	Die Ziele der EU-Richtlinie	4
2.3	Die wichtigsten Bestimmungen des HinSchG zusammengefasst.....	4
2.4	Gesetzmäßigkeit, regulative Standards und Kontrolle	6
3	<i>Die Pflicht</i>	7
3.1	Verpflichtete Unternehmen und Organisationen: wer, was, wann?	7
3.1.1	Betroffene Unternehmen.....	7
3.1.2	Meldestellen	7
3.1.3	Aktueller Umsetzungsstand Februar 2022	8
3.2	Meldekriterien: EU-Recht, nationales Recht, firmeninterne Regularien?	8
3.3	Hinweisgebersysteme: gesetzliche Anforderungen, Vorteile, digitale Nutzung.....	10
3.3.1	Gesetzliche Anforderungen:.....	10
3.3.2	Vorteile von digitalen Hinweisgebersystemen	10
4	<i>Die Chance - Nutzen und Vorteile im Unternehmen</i>	11
4.1	Praktische Umsetzung und Vorgehensweise	12
4.2	Motivation von Hinweisgebern – Erfahrungen aus der Praxis	13
4.3	Präventivmaßnahmen gegen Verfehlungen	14
4.4	Fazit.....	15
5	<i>Umsetzungsbegleitung</i>	16
5.1	Beratungsinhalte.....	16
5.2	Ergebnis	18

1 Überblick

Mit der EU-Whistleblower-Richtlinie, national umgesetzt im neuen Hinweisgeberschutz-Gesetz, beabsichtigt die EU den Schutz von Whistleblowern bei Meldungen zu Fehlverhalten in Betrieben und Organisationen, die für die Abgabe von Hinweisen künftig Meldesysteme mit bestimmter Ausgestaltung bereitstellen müssen.

Fehlverhalten kann sein: Verstöße gegen ethisch-moralische Grundsätze, EU-Recht, nationales Recht, doch auch gegen firmeninterne Regelungen. Das Gesetz gilt bereits für Unternehmen im Mittelstand ab 250 Mitarbeitern und nach einer Übergangsfrist ab 50 Mitarbeitern.

Regulative Standards schreiben Reaktionsfristen, Vertraulichkeit / Datenschutz und Ablaufprozesse für Meldesysteme vor in Bezug auf die Kommunikation zwischen Hinweisgebern und Hinweisempfängern, Ebenso gelten Vorschriften zu Information von Mitarbeitenden, revisions-sichere Dokumentation von Vorkommnissen und deren Bearbeitung wie auch die Interaktion zwischen den Beteiligten.

Wie ist nun ein Meldesystem als integrativer Bestandteil eines Compliance Management Systems umzusetzen? Welche Anforderungen, Pflichten und Chancen bringt die EU-Richtlinie mit sich und wie ist sie im Mittelstand umzusetzen?

2 Vorbemerkungen zum Hinweisgeberschutz – Gesetz- - Pflicht und Chance für Unternehmen -

2.1 Worum geht es?

Berichte über Missbrauch in öffentlichen und kirchlichen Einrichtungen, #metoo-Aktivitäten und Rassismus-Debatten bewirkten in den letzten Jahren zunehmend eine Sensibilisierung für Missbrauch, Diskriminierung und sexueller Belästigung, sei es in der Öffentlichkeit oder am Arbeitsplatz.

Aktuelle Vorkommnisse im wirtschafts- und finanzpolitischen Umfeld wie der Wirecard-Skandal, Cum Ex-Geschäfte, Manipulationsvorwürfe gegen Facebook oder die „Masken-Affäre“ machen schmerzhaft bewusst, wie stark Compliance Verstöße die Gesellschaft treffen und Vertrauen nachhaltig zerstören können.

Die Schäden daraus: finanzielle Verluste, schwere Vertrauensschäden in Organisationen, Reputationsverluste in der Öffentlichkeit, bei Kunden / Lieferanten u.v.m.

Aufgedeckt werden die Regelverstöße oft von mutigen Menschen, (ehemaligen) Mitarbeitenden oder sonstigen Betroffenen, die Rechtsverstöße, beobachtete und erlebte Geschehnisse nicht mit ihrem Gewissen vereinbaren können, intern kein Gehör finden bzw. Repressalien durch ihre Arbeitgeber befürchten.

Wenden sich Hinweisgeber hilfesuchend mit ihren Informationen direkt an Behörden oder an Medien, kann das entsprechende Folgen haben, sowohl für die Organisation wie auch für die Whistleblower persönlich:

Presserummel, Jobverlust, Reputationsverlust, Schadenersatzklagen, finanzielle Schäden – sofern diese nicht bereits durch die gemeldeten Vorkommnisse an sich entstanden sind – Gesichtsverlust in der Gesellschaft, auch für die Familie.

Gerade bei Offenlegung von Informationen, die im öffentlichen Interesse stehen, wie bspw. Berichterstattung zu mutmaßlichen Kriegsverbrechen und Korruption, wurden Existenzen zerstört, so geschehen im weltbekannten Fall von Julian Assange.

Die europäische Union hat nun zum Schutz von Hinweisgebern bereits Ende 2019 eine Richtlinie in Kraft gesetzt, die bis 17. Dezember 2021 von den Mitgliedsstaaten in nationales Recht umzusetzen war, was jedoch bislang nicht geschehen ist. Doch das Hinweisgeberschutz-Gesetz, auch „Whistleblower“-Gesetz, wird unabwendbar in Kürze in Kraft treten, bindend umzusetzen bereits für KMU ab 50 Mitarbeitenden.

2.2 Die Ziele der EU-Richtlinie

Die EU-Whistleblower-Richtlinie 2019/1937 regelt den Schutz natürlicher Personen, die im Rahmen ihrer beruflichen Tätigkeit selbst Schaden erfahren oder Informationen über Verstöße gegen EU-Recht erlangt haben und diese an interne oder externe Meldestellen weitergeben.

- Sie zielt darauf, einen europäisch ausgeglichenen Schutz zu gewährleisten und Hinweisgeber, die Missstände aus Unternehmen und Organisationen oder Rechtsverstöße offenlegen, besser als bisher vor Vergeltungsmaßnahmen zu schützen.
- Es gilt deren Identität zu wahren und Repressalien wie Entlassung, Degradierung, Anklage, Denunziation, Verleumdung bis hin zum beruflichen und privaten Bankrott zu vermeiden und ggf. zivil- oder strafrechtlich zu ahnden.
- Der Schutz der Hinweisgeber gilt für alle Meldungen, die in gutem Glauben abgesetzt werden; es wird Meldenden nicht auferlegt zu entscheiden, welches Recht nun denn auf den Hinweis anzuwenden ist.
- Weiterhin steht die Einführung der Beweislastumkehr zur Diskussion, d.h. der Arbeitgeber muss nachweisen, dass im Falle der Kündigung eines Mitarbeitenden und dem Hinweis auf Missstände keinerlei Verbindung besteht. Dies soll gleichermaßen für Angestellte Arbeitnehmer wie auch für Beamte gelten.
- Verstöße gegen geltendes Recht in und von Unternehmen soll rascher aufgedeckt und künftig präventiv unterbunden werden.

2.3 Die wichtigsten Bestimmungen des HinSchG zusammengefasst

Die regulativen-Standards ISO 37002 und ISO 37301 setzen klare Maßstäbe an effektive Meldesysteme und empfehlen als unternehmerische Grundlage für eine nachhaltig erfolgreiche Organisation ein wirksames Compliance-Managementsystem.

Welche Anforderungen an Meldesysteme gelten und wie sieht die Prozesskette Compliance Management aus?

Meldesysteme

- Arbeitgeber legen den Rahmen fest, in dem Verstöße oder Missstände melderrelevant sind: EU-Recht, nur deutsches Recht, oder auch organisationsinterne Richtlinien und geben damit Mitarbeitenden eine Ausrichtung
- Meldende haben die Wahl zwischen der Nutzung eines unternehmensinternen oder eines behördlichen Meldesystems im ersten Schritt, bevor sie sich mit Hinweisen gegen Regelverstöße an die Öffentlichkeit wenden
- Unternehmen und Organisationen sind verpflichtet, interne Hinweisgebersysteme einzurichten, die Mitarbeitenden die (anonyme) Meldung von Regelverstößen ermöglichen
- Behörden müssen ebenfalls sog. öffentliche Meldestellen einrichten, damit Hinweisgeber ihr Wahlrecht ausüben können

Whitepaper zur Whistleblower-Richtlinie und Compliance Management

- Die Wahrung der Anonymität des Whistleblowers wie auch der im Mittelpunkt der Meldung stehenden Person(en) hat Priorität
- Für die Reaktion auf abgegebene Hinweise sind von den Hinweisnehmern verbindliche



Fristen für Eingangsbestätigung und Beantwortung einzuhalten (7 Tage / 3 Monate); ob jedoch die Bearbeitung von anonymen Hinweisen umfänglich oder eingeschränkt verpflichtend ist, bleibt in der Umsetzung im dt. Recht abzuwarten

- Für die Entgegennahme von Meldungen müssen Hinweisgebern vom Unternehmen unparteiische Personen genannt werden, die 24/7 Hinweise (persönlich oder digital) annehmen und weiterbearbeiten können
- Für Meldesysteme und die damit verbundenen Prozesse gelten Datenschutzvorgaben zum Schutz der Identitäten wie zur Speicherung und Löschung von Daten. Es zählen Dokumentations- u. revisionssichere Archivierungspflichten, d.h. Aufzeichnungen und der Meldekanal sind vor Zugriffen Dritter und unbefugter Personen zu schützen.

Grundlegende Elemente eines Compliance Management Systems:

Vorbeugen → Erkennen → Reagieren → Anpassen praktisch umgesetzt:

- Anwendungsbereiche, Compliance-Politik, Rollen und Verantwortlichkeiten sind festzulegen und auf allen organisatorischen Ebenen verpflichtend umzusetzen
- Führungskräfte und Mitarbeitende sind inhaltlich und organisatorisch im Umgang mit dem Meldesystem und eingehenden Hinweisen zu informieren und regelmäßig zu schulen, erworbenes Wissen ist abzufragen
- Fehlverhalten melden, erkennen, beurteilen, bearbeiten und reagieren unter Einhaltung rechtlich vorgegebener Fristen, und das DSGVO-konform, ist die Verpflichtung
- Evaluierung, Bewertung und Kontrolle des Compliance-Management-Systems CMS wird verlangt

Whitepaper zur Whistleblower-Richtlinie und Compliance Management

- Anpassungen sind, falls durch Erkenntnisse erforderlich, im Sinne der permanenten Verbesserung vorzunehmen
- Verwaltung, Dokumentation, Teilen von Informationen, Archivierung / Dokumenten-Management sind entsprechend zu etablieren.

2.4 Gesetzmäßigkeit, regulative Standards und Kontrolle

Für Leitungsorgane stellen sich folgende Fragen:

- Ist die Richtlinie verpflichtend umzusetzen?
- Welche Behörde kontrolliert und ahndet Verstöße?
- Wie ist im Falle des Hinweisgeberschutzes die Zuständigkeit f. behördliche Meldestellen geregelt?

Kann- oder Muss-Bestimmung?

Die EU-Richtlinie ist von den Ländern umzusetzen in ein nationales Hinweisgeberschutz-Gesetz, demgemäß verpflichtend für die betroffenen Organisationen.

Nicht-Einhaltung der Vorschriften für Organisationen ist nach dem Ordnungswidrigkeitengesetz bußgeldbewehrt und wird von der zuständigen Verwaltungsbehörde überwacht; dies werden voraussichtlich die zuständigen Gewerbeaufsichtsämter sein, sofern Unternehmen / Organisationen nicht unter eine Spezialzuständigkeit fallen.

Über die Höhe von Strafen darf noch spekuliert werden.

Zuständigkeit externer Meldestellen:

Diskutiert wird die Zuständigkeit für externe Meldestellen, die beim Bundesdatenschutz-beauftragten angesiedelt sein kann, wohingegen bei Verstößen gegen Rechnungslegung oder Buchführungsregeln, Aktionärsrechte oder Ähnliches die BaFin als externe Meldestelle fungieren kann. Jedermann kann dorthin Verstöße melden und die Behörde muss den Meldungen dann nachgehen.

Regulative Standards zur Whistleblowing-Richtlinie u. Compliance-Standards zur Vertiefung:

ISO 19600/37301;

DIN ISO 37001 Compliance Managementsysteme – Anforderungen u. Leitlinien

DIN ISO 37002 Whistleblowing Management – Systeme – Leitlinien

DIN ISO 31000 Risikomanagement-Leitlinien

DIN ISO 37001 Managementsysteme zur Korruptionsbekämpfung

3 Die Pflicht

3.1 Verpflichtete Unternehmen und Organisationen: wer, was, wann?

3.1.1 Betroffene Unternehmen

Da EU-Recht (Unionsrecht) Teil unseres täglichen (Wirtschafts-)Lebens ist, sind alle in der untenstehenden Grafik genannten Unternehmen innerhalb der EU von der Richtlinie betroffen, jeweils in der nationalen Rechtsauslegung.

Für Banken, Versicherungen und börsennotierte Aktiengesellschaften sind interne Meldesysteme und Compliance-Regularien schon lange verpflichtend. Unternehmen des Mittelstandes müssen sich nun auch dem Hinweisgeberschutz stellen, indem sie die EU-Verordnung zu Compliance-Themen zeitnah umsetzen: im Mittelstand bei einer Unternehmensgröße ab 50 Mitarbeitern, bei Behörden, Gemeinden und öffentlichen Einrichtungen unabhängig von der Mitarbeiterzahl:

Betroffene des Hinweisgeberschutzgesetzes (HinSchG)	
Öffentliche Stellen	Private Unternehmen
> alle juristischen Personen des öffentlichen Rechts	> Unabhängig von Branche u. Rechtsform
> Ausnahmen können gelten für:	> Ab 50 Beschäftigten (Kopfzahl) unabhängig vom Jahresumsatz
* öffentliche Stellen mit < 50 Mitarbeitenden	> Unternehmen in der Finanzdienstbranche ausnahmslos
* Gemeinden mit < 10.000 Einwohnern	
Besonderheiten:	Besonderheiten:
>> Regelungen im Landesrecht:	> Unternehmen ab 50 bis 249 Mitarbeitenden können sich Ressourcen für Entgegennahme und Untersuchung von Hinweisen teilen
> Meldekanäle dürfen von gemeinsamen Behörden-diensten betrieben werden	
> Gemeinden können sich interne Meldekanäle teilen	aber: Jede Unternehmenseinheit benötigt einen separaten Meldekanal

3.1.2 Meldestellen

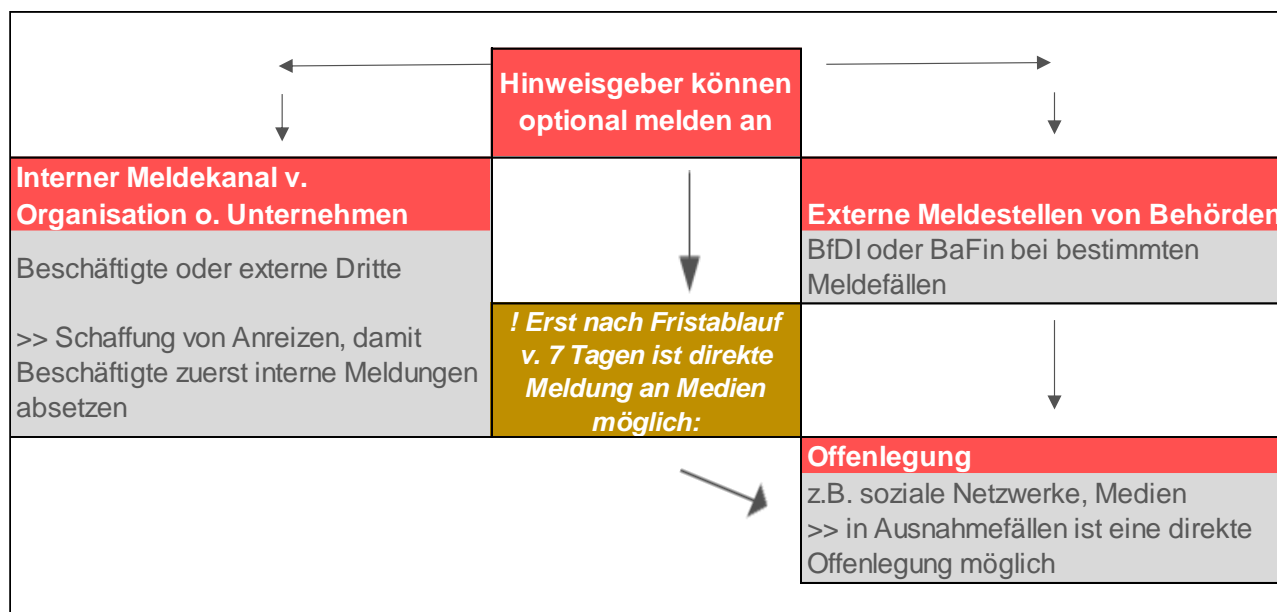
An welche Stellen können Hinweise gemeldet werden?

Hinweisgeber können wählen, ob sie im ersten Schritt den angebotenen internen Meldekanal ihres Arbeitgebers nutzen oder die Meldestelle einer Behörde. Die unternehmensinterne Meldestelle wird der Whistleblower sicher nur nutzen, wenn er auf Diskretion und Anonymität vertrauen kann im Hinblick auf die hinweisnehmenden Personen und das Vertrauen auf Schutz seiner

Whitepaper zur Whistleblower-Richtlinie und Compliance Management

Identität, Einhaltung der Vorschriften und ohne berufliche u. private Nachteile in Kauf nehmen zu müssen.

Erst wenn innerhalb der vorgeschriebenen Fristen weder vom Unternehmen noch von der Behörde eine Reaktion erfolgt, darf der Hinweisgeber sich direkt an die Öffentlichkeit, Medien oder soziale Netzwerke, wenden.



3.1.3 Aktueller Umsetzungsstand Februar 2022

Die Richtlinie hätte bis Dezember 2021 in nationales Recht umgesetzt werden müssen, doch die Umsetzungsfrist ist in Deutschland verstrichen. National agierende Unternehmen bewegen sich auf unsicherem Terrain, da die Richtlinie in einigen EU-Staaten fristgerecht umgesetzt wurde, in anderen dagegen nicht.

Zwar sieht der neue Koalitionsvertrag der Ampel-Regierung eine zügige, rechtssichere und praktikable Umsetzung vor – Stand November 2021– sogar über die EU-Regeln hinausgehend, gibt jedoch keinen konkreten Termin an. Die Umsetzung wird jedoch zeitnah erfolgen und der Detaillierungsgrad der bisher überschießenden Formulierung im deutschen Gesetz bleibt bis dahin offen.

3.2 Meldekriterien: EU-Recht, nationales Recht, firmeninterne Regularien?

Welche Meldekriterien sind relevant? Verstöße gegen EU-Recht bzw. deutsches Recht, oder auch Verstöße, die im Focus des öffentlichen Interesses sind? Firmeninterne Regularien?

Whitepaper zur Whistleblower-Richtlinie und Compliance Management

Die Richtlinie geht zunächst von Verstößen gegen geltendes EU-Recht aus wie Datenschutzrecht, Wettbewerbsrecht, Konsumentenschutz, Produktsicherheit, Steuerrecht, Umweltschutz, u.v.m.

- ⇒ **Die Meldeinhalte können von Unternehmen u. Organisationen festgelegt werden: nur EU-Recht, zusätzlich Verstöße gegen nationales Recht, zusätzlich Compliance-Richtlinien der Organisation.**

Das deutsche Hinweisgeberschutz-Gesetz ahndet voraussichtlich Verstöße gegen rein nationales Recht; diskutiert wird der Schutz sogar bei „erheblichen Verstößen gegen Vorschriften sowie sonstigem Fehlverhalten, dessen Aufdeckung im besonderen öffentlichen Interesse liegt“.

Beispiele für deutsche Rechtsverordnungen ...:

- Arbeitsschutz
- Datenschutz-Grundverordnung
- GOBD
- Geldwäsche-Gesetz
- Geschäftsgeheimnisgesetz
- Lieferkettengesetz
- Steuergesetze und -Standards wie IdW PS 340, IKS, Integriertes Risikomanagement
- StaRUG ... und zahlreiche weitere Gesetze, die ein Betrieb beachten muss

... und betriebliche Spannungsfelder...:

... wie IT-Sicherheit, Diebstahl, Korruption, Unterschlagung, Wettbewerbs- und Marktrisiken, strategische Risiken, Nachhaltigkeitsregeln, Umweltschutz und CO²-Standards, zu denen Verfehlungen als relevante Meldekriterien dienen können.

Über die gesetzlichen Vorschriften hinaus haben Unternehmen oft noch eigene „Gesetze“, Firmenrichtlinien wie festgelegte Werte, Verhaltens-Codices, eine Art freiwillige Selbstverpflichtung, fixiert in den Compliance-Richtlinien, deren Verletzung ebenfalls ein Meldekriterium sein kann.

3.3 Hinweisgebersysteme: gesetzliche Anforderungen, Vorteile, digitale Nutzung

Welche Kriterien muss ein Hinweisgebersystem erfüllen, um den kommenden gesetzlichen Anforderungen zu genügen?

3.3.1 Gesetzliche Anforderungen:

Der Gesetzgeber fordert ein Meldesystem, das Hinweisgebern ermöglicht

- Schriftlich
- Mündlich und
- Persönlich Meldungen abzusetzen,
- Rund um die Uhr und ohne sprachliche Barrieren

Meldungen müssen innerhalb einer 7-Tagesfrist bestätigt und innerhalb von 3 Monaten bearbeitet werden. Dazu bedarf es der Kommunikation eines unparteiischen Hinweisnehmers mit dem Hinweisgeber, der revisionssicheren und im Zweifelsfalle gerichtsfähigen Dokumentation von Hinweis und Weiterbearbeitung sowie der Archivierung und dies unter Beachtung datenschutzrechtlicher Aspekte.

Spätestens hier stellt sich die Frage, ob kleine Mittelständler all diesen Anforderungen gewachsen sind, evtl. über eine Compliance-Abteilung verfügen und eine unparteiische geeignete Person als Hinweisnehmer stellen können.

Alternativen sind Outsourcing der Prozesse an externe Anbieter wie Servicegesellschaften/Compliance Offices und die Einführung eines digitalen Meldesystems.

3.3.2 Vorteile von digitalen Hinweisgebersystemen

Ausgewählte Anbieter bieten digitale Meldesysteme an, die den gesetzlichen Anforderungen genügen und in Unternehmen komfortabel zu etablieren und zu betreiben sind.

Die Vorteile liegen auf der Hand:

- ✓ einfache Handhabung, 24/7 Verfügbarkeit, Mehrsprachigkeit
- ✓ Fristen- u. Dokumentenmanagement
- ✓ sichere Datenverarbeitung
- ✓ geringer lfd. Aufwand

Ein organisationseigenes internes Meldesystem und eine unparteiische Anlaufstelle erhöhen das Vertrauen und die Wahrscheinlichkeit, dass ein potenzieller Hinweisgeber die interne Meldestelle einem behördlichen Meldesystem vorzieht; auch ermöglicht es dem Arbeitgeber die interne Bearbeitung von Vorfällen, bevor Verstöße an die Öffentlichkeit geraten.

Das Angebot der Möglichkeit, Hinweise anonym abzugeben, ist nicht zu unterschätzen.

Whitepaper zur Whistleblower-Richtlinie und Compliance Management

Auch wenn die Bearbeitung von anonym erteilten Hinweisen gesetzlich nicht oder nur eingeschränkt gefordert werden wird, finden damit potenzielle Hinweisgeber eine vertrauensvolle Basis für die Nutzung interner Meldekanäle, bevor sie externe Systeme nutzen.

So zeigt der Whistleblowing-Report 2021 der EQS-Group mit der FH Graubünden auf, dass 73,2% d. Hinweisgeber sich für eine anonyme Meldung entscheiden, sofern diese Option verfügbar ist.

4 Die Chance - Nutzen und Vorteile im Unternehmen

Wer am Markt erfolgreich sein will, muss rechtliche, professionelle und gesellschaftliche Regeln einhalten. Öffentlichkeitswirksame CSR-Maßnahmen lancieren, aber Steuern hinterziehen und Umweltschäden begehen, tragen nicht zur Glaubwürdigkeit von Organisationen bei.

Unternehmen, die gegensteuern und nachweislich ethisch wie nachhaltig handeln, erhalten ihre Glaubwürdigkeit und gewinnen an Image und Wettbewerbsvorsprung.

Ein etabliertes Hinweisgebersystem, in das Mitarbeitende eingewiesen sind, bietet viele Vorteile:

- ermöglicht gleichzeitig Aufklärung von unternehmensbezogenem Fehlverhalten (moralisch/ethisch/arbeitsvertraglich ...) wie auch die Entdeckung von sog. Innentätern, die Unternehmen deutlichen Schaden zufügen können
- schützt Hinweisgeber und betroffene Personen durch die Möglichkeit der anonymen Meldung
- schützt Unternehmen finanziell vor Schäden u. Schadensersatzzahlungen und vor allem vor Reputationsverlust
- erhöht die Chancen für eine interne Behandlung der gemeldeten Themen ohne Einschaltung einer Behörde, d.h. das Unternehmen / die Organisation behält die Kontrolle über das Verfahren
- erhöht die Chancen zeitnah aus interner oder auch externer Quelle von Verfehlungen zu erfahren
- dient gelegentlich als Kummerkasten für Mitarbeiter, bietet jedoch gleichzeitig Achtungspotential für die Unternehmensentwicklung im Hinblick auf Hinweise zum Verstoß gegen interne Richtlinien und ethisch-moralische Gebote wie auch sonstige Schwächen
- stärkt das Unternehmen als Arbeitgebermarke
- fördert das Image bei den Beschäftigten, Geschäftspartnern und der Öffentlichkeit als ethisches und integriertes Unternehmen

Hinweisgeber können mit relevanten Meldungen gegen Verstöße und interne Richtlinien für den Erhalt der Unternehmenskultur wirken, oft sogar für die Vermeidung von Strafen und persönlicher Haftung der Firmenlenker.

Doch mit der Einführung eines (digitalisierten?) Meldesystems ist es nicht getan, für eine zukunftsgerichtete Organisation bedarf es der Einbindung des Hinweisgeberschutzes in wirkungsvolle Compliance-Strukturen.

4.1 Praktische Umsetzung und Vorgehensweise

Wie setzt man das Hinweisgeberschutz-Gesetz richtig und effektiv um?

Wie können sich Organisationen auf das kommende Gesetz vorbereiten?

Was gilt es zu beachten?

- **Unternehmenswerte**

Zunächst bedarf es des klaren Bekenntnisses der Geschäftsführung zu einer Vertrauenskultur und der Verankerung von Werten in einem Verhaltenskodex innerhalb des betrieblichen Compliance-Systems.

- **Interner Meldekanal**

Die Auswahl für ein eigenes rechtskonformes Hinweisgeber-Meldesystems sollte unter Berücksichtigung von Datenschutz und -Sicherheit, Dokumentations- und Archivierungs-möglichkeiten getroffen werden. Anonyme Meldungen müssen möglich sein, wohingegen eine Verpflichtung zu deren Bearbeitung in der EU-Richtlinie nur eingeschränkt vorgesehen ist.

Nicht zu vergessen: Einbindung des Betriebsrates, sofern installiert!

- **Hinweisempfänger**

Dabei ist die Festlegung eines unparteiischen Hinweisnehmers entscheidend, damit Whistleblower auch vertrauensvoll den internen Meldekanal dem behördlichen vorziehen. Dies können sein der Betriebsrat, ein HR-Leiter*in, ein Compliance-Manager*in, ein Firmenjurist*in oder eine externe Ombudsperson oder eine ausgelagerte Gesellschaft, ein Compliance Office.

- **Datenschutz und Vertraulichkeit**

Begleitend ist im Unternehmen der sorgfältige Umgang mit eingehenden Meldungen unter Wahrung der Identität von Hinweisgebern und von der Meldung betroffener Personen zu regeln; dies gilt auch während der gesamten Bearbeitungszeit des Vorfalls, soweit dies möglich ist.

- **Prozesse – interne Organisation - Verantwortlichkeit**

Wichtig ist die Festlegung der Verantwortlichkeiten im Betrieb mit Focus auf Fristen, Reaktion, Verwaltung und Dokumentation eingehender Hinweise und deren Bearbeitung.

Hierfür bedarf es der Erarbeitung einer Prozesskette mit Handlungsmaßnahmen, Relevanzbeurteilung, Eskalationsstufen, einer Kontrollinstanz, eines Verantwortlichen oder Ausschusses zur Analyse und Überwachung von Fällen und natürlich der umfassenden Dokumentation und Archivierung, und dies revisionssicher und gerichtsfähig.

Whitepaper zur Whistleblower-Richtlinie und Compliance Management

• **Information und Kommunikation**

... unter Mitarbeitern und Führungskräften und die behutsame, begleitete Einführung bzw. Anpassung vorhandener Compliance-Strukturen sind klärend, vorbereitend, vertiefend und können bereits präventiv wirken.

• **Outsourcing Meldesystem und Compliance-Management**

Sind Kapazitäten und / oder Kompetenz in der Organisation nicht darstellbar, empfiehlt sich die Nutzung eines externen Anbieters für Meldesystem und evtl. auch digitale Schulungs-Tools.

4.2 Motivation von Hinweisgebern – Erfahrungen aus der Praxis

Whistleblower - Helden oder Nestbeschmutzer?

Erfahrungen aus der Praxis

Nicht alle Unternehmer sind von der bevorstehenden Einführung des Gesetzes begeistert und sehen oft mehr Risiken als Vorteile. Aussagen wie „züchte ich mir damit Spione im eigenen Unternehmen?“ sind oft zu hören.

Wer entlarvt, gilt oft als Nestbeschmutzer. Nicht selten steht auch der eigene Ruf auf dem Spiel, denn manchmal wird Whistleblowern Neid oder Missgunst unterstellt. Ist das wirklich so?

Im Gegenteil:

Für manche Whistleblower ist das Aufdecken von Pflichtverstößen eine Gewissensfrage, andere wollen Gerechtigkeit oder handeln aus Pflichtbewusstsein. Dabei sind Hinweisgeber sehr couragierte Menschen: sie riskieren nicht nur Nachteile für ihre Karriere und ihre Familie, sondern müssen auch mit Schadensersatzklagen und übler Nachrede rechnen.

Zwar gebe es vereinzelt Hinweisgeber, die Kollegen und Führungskräfte anschwärzen, um ihnen zu schaden, doch nach Aussage von Studien und Erfahrungsberichten sei das wohl eher die Ausnahme. Offensichtlich sind gemeldete Verstöße überwiegend relevant, der Missbrauch des Meldesystems ist in Deutschland- die absolute Ausnahme, doch sind erst wenige Meldesysteme eingerichtet.

- Laut einer Studie der TH Chur zusammen mit dem Softwareanbieter EQS verfügten im Jahr 2019 lediglich 5% der befragten Unternehmen über eingerichtete Meldestellen, mittlerweile sicher mehr.
- „Rund 90% der Hinweisgeber versuchen zunächst intern, die beobachteten Missstände anzusprechen, bevor sie sich an Behörden, Medien oder die Öffentlichkeit wenden – vorausgesetzt sie finden im Unternehmen geeignete Kanäle und eine offene Kultur vor.“

(Quelle: Whistleblowing-Report 2021 EQS & FH GR).

Whitepaper zur Whistleblower-Richtlinie und Compliance Management

- Gemäß Whistleblowing-Report 2021 setzen rund 73% der Hinweisgeber ihre Meldungen anonym ab, sofern diese Option besteht, aus Unsicherheit vor den Konsequenzen und Unkenntnis der weiteren Vorgehensweise, wobei die verpflichtende Bearbeitung von anonym eingehenden Hinweisen nur eingeschränkt vorgeschrieben ist. Allerdings zeigen Untersuchungen, dass die Zahl der wertvollen Meldungen sich mit der Sicherheit der Anonymität erhöht, was Unternehmen proaktives und frühzeitiges Handeln ermöglicht und Risiken minimiert.
- Kategorien eingehender Meldungen sind meist:
 - rechtswidriges / strafbares Verhalten von Mitarbeitern und Dritten
 - Mitarbeiterthemen, HR-bezogen, wie Mobbing durch Kollegen u. Vorgesetzte, Verstöße gegen arbeits- bzw. vertragsrechtliche Bestimmungen etc.

Demnach sind beabsichtigte Denunziationen kaum vorgekommen und die eingehenden Meldungen für Unternehmensentwicklung und Personalpolitik eher wertvoll zu sehen.

Quelle: Whistleblowing-Report 2021 FH Graubünden und EQS-Group

4.3 Präventivmaßnahmen gegen Verfehlungen

Was können Organisationen präventiv tun, um Rechtsverstöße und Verfehlungen zu vermeiden?

An dieser Stelle sei die Empfehlung ausgesprochen, in der Organisation zusammen mit den Führungskräften und Mitarbeitern relevante Themen und Rechtsverordnungen wie auch eigene Unternehmenswerte zu erarbeiten und Meldeinhalte entsprechend zu fixieren. Erfahrungsgemäß ist ein Hinweisgebersystem insbesondere dann erfolgreich, wenn es in eine transparente und vertrauensvolle Unternehmenskultur eingebettet ist.

Wir raten Unternehmen daher rechtzeitig die Etablierung eines professionellen Compliance-Management-Systems (CMS) und die Einbindung eines eigenen internen, evtl. digitalen Meldesystems, um die Meldungen von Whistleblowern über externe Meldekanäle zu vermeiden.

Sind Mitarbeiter und Führungskräfte zu den Anforderungen des Hinweisgeberschutz-Gesetzes entsprechend sensibilisiert und informiert, werden sie wiederkehrend geschult, werden Auflagen und Firmenregeln hinreichend kommuniziert und ist eine entsprechende Prozesskette etabliert, ist das Unternehmen gerüstet für das Inkrafttreten des Schutzgesetzes.

4.4 Fazit

Bekannt sich die Firmenleitung zu einer vertrauensvollen Unternehmenskultur und wird diese gelebt, kann mit Sicherheit der professionelle Einsatz von digitalen Hinweisgebersystemen und die Verankerung in einer betrieblichen Compliance-Struktur zahlreiche Verstöße und Skandale aufklären oder gar präventiv verhindern. Die Erfahrung, dass Whistleblower keine Denunzianten sind, sondern mit Überwindung ihr Wissen preisgeben, wird künftig die Einstellung verändern und zahlreiche Abläufe und Prozesse auf den Prüfstand stellen.

Der beabsichtigte umfassende EU-einheitliche Hinweisgeberschutz wird künftig zur unternehmerischen Normalität werden. Er ist Ausdruck einer offenen zukunftsorientierten Kultur, soll dauerhaft einen Sinneswandel in vielen Unternehmen auslösen und die verbindliche Einrichtung von professionellen Compliance-Strukturen zur Folge haben, wie sie in Konzernen und in der Finanz- und Versicherungswirtschaft seit langem üblich und etabliert sind. Denn werden relevante Rechtsverstöße vertuscht, so ist das betriebswirtschaftlich, volkswirtschaftlich wie auch ethisch/moralisch problematisch. Je nach Sachlage werden Gelder ineffizient verschwendet, Menschen leiden, Mitarbeitende und ihre Familien, Kunden, Bürger, Steuerzahler, Aktionäre sind von den Folgen betroffen.

Unabdingbar sind die umfassende Information, Sensibilisierung und Kommunikation innerhalb eines Unternehmens für Führungskräfte und für Mitarbeitende, ebenso wie die Einbindung des Hinweisgeberschutzes in ein bestehendes oder neu zu erarbeitendes Compliance-Management-System (CMS) im Gesamtkontext der nachhaltigen Betriebsführung, Weiterentwicklung und Wettbewerbsfähigkeit einer Organisation.

Auch wenn die EU-Richtlinie bis zum heutigen Tage für Deutschland nicht umgesetzt wurde, empfehlen wir Unternehmen, nicht bis zum letzten Tag damit zu warten und dann einen Kaltstart hinzulegen, sondern sich und ihre Organisation vorzubereiten und die Umsetzung der EU-Whistleblower-Richtlinie zeitnah anzugehen.

Jedes Unternehmen, gerade wenn es international agiert, sollte sich die Chancen eines internen organisationsweiten Meldesystems vor Augen führen.

Von Karin Scherer / Scherer Concept
www.scherer-concept.de

5 Umsetzungsbegleitung

Welche Unterstützung können wir Ihnen bieten in der Umsetzung des Hinweisgeber-schutz-Gesetzes?

Mit der vom Gesetzgeber initiierten Einführung eines Meldesystems als Grundlage einer gelebten Vertrauenskultur bedarf es der Integration des Hinweisgeberschutzes in eine wertschätzende Unternehmenskultur.

Dazu gehört die Erarbeitung von Unternehmenswerten und -Richtlinien, das Bewusstsein über rechtliche, soziale und gesellschaftliche Verpflichtungen, die umfassende Aufklärung in der Organisation sowie permanente Kommunikation auf Führungs- wie auch auf Mitarbeiterenebene.

5.1 Beratungsinhalte

Unsere Leistungen

Compliance Beratung und Umsetzung des Hinweisgeberschutzes:

Wir erarbeiten mit Unternehmen und Organisationen ein komplettes Compliance Management System unter Einbindung von Führungskräften der verschiedenen Ebenen sowie von Betriebsrat und Datenschutzbeauftragten:

1. Compliance-Grundlagen und Leitlinien

- Begriffsverständnis, Definition u. Beschreibung des Anwendungsbereiches und der Einflussfaktoren
- Überprüfung und ggf. Aktualisierung existenter Leitlinien
- Grundanforderungen an das CMS
 - Zielsetzung
 - Strukturaufbau
 - Prozessaufbau
- Erarbeitung der Unternehmenskultur / der unternehmerischen Werte:
 - ethisch-moralische Werte,
 - eigene Regularien u. Ziele wie bspw. Mitarbeiterführung, Nachhaltigkeit
- Ausarbeitung der Compliance Kultur, Festlegung der Grundlagen, Formulierung des Code of Conduct / Ehrenkodex

2. Festlegung von Interessensgruppen und Funktionsträgern im Unternehmen – (*Großunternehmen vs. KMU*)

- Oberste Leitung / Führungsorgane, HR-Management, Compliance Team
- Interessensgruppen und deren Anforderungen / Erwartungen an die Organisation

3. Risikobereiche und Rechtskonformität

- Identifizierung der Risikobereiche, Erarbeitung des Rechtskatasters (weitgehend festgelegt durch WBRL)
- Rechtskonformität / Einhaltung geltender Verordnungen / Gesetze,
- Einschätzung u. Bewertung der Risiken, Abschätzung der Konsequenzen für das Unternehmen bei Rechtsverstößen
- Bestimmung Verantwortlicher und wirksame Pflichtenübertragung

An dieser Stelle stellt sich die Frage:

➔ Inhouse-Lösungen oder Outsourcing an Servicegesellschaft?

4. Organisation und Prozesse – (*Großunternehmen vs. KMU*)

- Erarbeitung von Prozesse und Organisation für Zuständigkeiten, Berichtswege, Kommunikation intern / extern / mit Hinweisgebern,
- Dokumentation / Archivierung, Versionskontrolle etc.,
- *Festlegung von Meldekanälen* ➔ *Auswahl Hinweisgebertool*
- *Festlegung von Meldeprozessen* ➔ *unparteiische Hinweisnehmer / Ombudspersonen*
- Organisation der Untersuchungsprozesse ➔ Beurteilung d. Relevanz, erste juristische Einschätzung der Lage und erforderlichen Maßnahmen
- Abwägung von Interessenskonflikten
- Kommunikationsaktivitäten intern / extern / mit Hinweisgebern
- Revisionssichere und gerichtsfähige Dokumentation
- Simulation von Eskalationsstufen und Reaktionsverhalten
- Erfahrungsaustausch / Lenkungssitzungen, ggf. Anpassung von Organisation und Prozessen

5. Information, Kommunikation, Schulung

Schulungs-Tools für Führungskräfte und Mitarbeiter, Angebot eines „Compliance-Führerschein“

6. Einbindung der Lieferkette - Lieferantenkodex

- Lieferantencodices formulieren und kommunizieren
- Lieferanten u. Mitarbeiter im Umgang mit Lieferanten einweisen
- Einhaltung von Lieferantenrichtlinien überwachen

7. Systemüberwachung, -Analyse und Verbesserung von CMS und Meldesystem

- Etablierung und Durchführung von Steuerkreissitzungen (Teilnehmer, Aufgaben)
- Tauglichkeit, Überwachung u. Bewertung des Systems und der Tools
- Erfordernis von Verbesserungen und weiterer Präventivmaßnahmen
- Zertifizierung / Audit?

8. Berichtswesen

- Compliance-Bericht
- Managementbewertung
- Zertifizierung
- Maßnahmen

5.2 Ergebnis

Mit der Etablierung des Hinweisgeberschutzes und eines werte- und prozessorientierten Compliance Management Systems im Sinne einer wirksamen Kontrolle gegen Zuwiderhandlungen erhalten Unternehmen und Organisationen die Sicherheit,

- alle relevanten Gesetze und Vorschriften einzuhalten und dauerhaft zu erfüllen
- Haftungsrisiken, Strafzahlungen und Schadensersatzklagen für Führungskräfte zu verhindern
- Reputationsschäden zu vermeiden
- Wertvolle Arbeitskräfte zu gewinnen und zu halten
- Kunden und Lieferanten zu überzeugen und zu binden
- Transparenz und durchgängige Verhaltensrichtlinien für die gesamte Organisation zu schaffen

Darüber hinaus werden Unternehmenswerte, ethisch-moralische Verhaltens-Codices und interne Compliance-Richtlinien erarbeitet und etabliert, zusammen mit Mitarbeitern und Führungskräften, als Basis für das Entstehen einer Vertrauenskultur.

Karin Scherer

Nachhaltigkeits- u. Compliance Manager, Datenschutzbeauftragte

karin.scherer@scherer-concept.de

mobil: +49 (0)171 - 14 63 916

Whitepaper zur Whistleblower-Richtlinie und Compliance Management

Karin Scherer ist selbständige Unternehmensberaterin in der Scherer GmbH und daneben als Consulting Partnerin für ausgewählte Beratungsgesellschaften für die mittelständische Wirtschaft projektbezogen tätig. Sie hat mehr als 20 Jahre Erfahrung als geschäftsführende Gesellschafterin eines mittelständischen Handels- und Handwerksbetriebes der Automobilwirtschaft mit den Schwerpunkten Finance/Controlling, Sales/After Sales und Personalmanagement.

Karin Scherer studierte an der FAU Erlangen-Nürnberg und an der JWG-Univ. Frankfurt/Main Betriebswirtschaft, später an der GSO-HS Nürnberg Restrukturierung/Sanierung und ist ausgebildet als Datenschutzbeauftragte beim TÜV Süd, Compliance- u. Nachhaltigkeitsmanagerin und Beraterin bei Alchimedus © und als Mental Coach.

