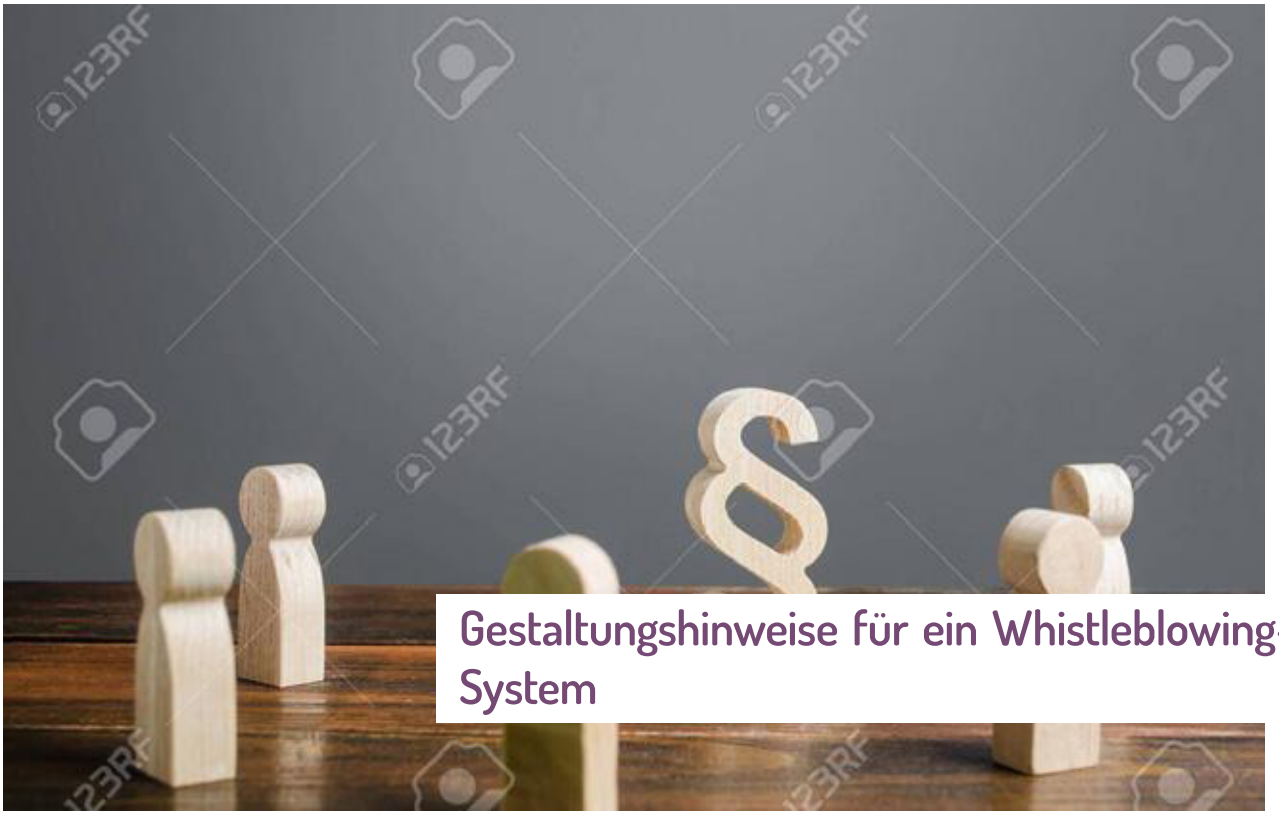

Gestaltungshinweise für ein Whistleblowing-System

Die Tragweite von Whistleblowing-Systemen zeigte eine Anhörung vor dem US-Kongress im Dezember 2019. Es ging um die Abstürze von zwei Boeing 737 Maschinen. 346 Menschen haben dabei ihr Leben verloren. Ein ehemaliger Boeing-Angestellter hatte vor dem ersten Absturz schwerwiegende Bedenken über die Fertigungsqualität geäußert und vor dem zweiten Unglück erneut Probleme an ranghohe Boeing-Führungskräfte gemeldet. Die Hinweise haben nichts bewirkt. In Deutschland rücken die Compliance-Pflichten durch Skandale wie Wirecard, Cum-Ex oder Dieselgate in den Fokus. Im Hinblick auf das kommende Verbandssanktionengesetz sollten auch mittelständische Unternehmen ihre Compliance-Maßnahmen intensivieren.

Compliance-Management-Systeme

Die Geschäftsführung hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen. Erforderlich sind angemessene, an der Risikolage des Unternehmens ausgerichtete Maßnahmen. Von Bedeutung ist, inwieweit das Unternehmen der Verpflichtung genügt, Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden, und ob das Unternehmen ein angemessenes und wirksames Compliance-Management-System (CMS) installiert hat.[1] Die Anforderungen an ein CMS lassen sich wie folgt zusammenfassen:

1) Nach dem Prinzip "Tone from the Top" müssen Mitarbeiter spüren, dass Compliance von ganz oben getragen wird.
2) Compliance verlangt eine regelmäßige straf- und ordnungswidrigkeitenrechtliche Risikoanalyse, die eine Vielzahl von Rechtsgebieten betreffen kann, z. B. Anti-Korruption, Kartellrecht, Geldwäsche, Produktsicherheit oder Datenschutz.
3) Hinweisgebersysteme und Compliance-Ombudsleute sind unverzichtbare Elemente eines funktionierenden CMS. Mitarbeiter und evtl. auch Unternehmensexterne müssen die Möglichkeit haben, eine anonyme Meldung – jenseits des klassischen Hierarchieweges – abzugeben. Ein solches System ist als eine der zentralen Erkenntnisquellen über Compliance-Verstöße die Herzkammer eines wirksamen Compliance-Managements. Hinweisgebersysteme werden mit Umsetzung der EU-Whistleblower-Richtlinie (WBRL) im Dezember 2021 weiter an Bedeutung gewinnen. Alle Unternehmen mit mehr als 50 Beschäftigten, juristische Personen des öffentlichen Sektors und Gemeinden ab 10.000 Einwohnern werden nach Artikel 8 WBRL dann verpflichtet, zuverlässige Meldekanäle einzurichten.[2]
4) Schließlich müssen Compliance-Verstöße aufgeklärt und konsequent geahndet werden. Es gilt die Pflichtentrias: „Aufklären, Abstellen, Ahnden". Folgende Regelungen sind für ein Whistleblowing-System wichtig:

Meldungen, Dokumentation und Vertraulichkeitsgebot

Hinweisgeber können bei Verdacht auf Compliance-Verstöße Fehlverhalten von allen Mitarbeitern und Führungskräften melden. Compliance-Verstöße sind Straftaten oder Ordnungswidrigkeiten, die aus

1 BGH, Urteil vom 9.5.2017 – 1 StR 265/16

2 vgl. grundlegend: Ninon Colneric und Simon Gerdemann, Die Umsetzung der Whistleblower Richtlinie in deutsches Recht, HSI-Schriftenreihe Band 34, Frankfurt am Main 2020

Dr. Burkhard Fassbach (Rechtsanwalt) und Dr. Frank Hülsberg (Wirtschaftsprüfer), Warth & Klein Grant Thornton AG

der Organisation des Unternehmens heraus begangen werden, sich gegen Dritte, die öffentliche Ordnung oder gegen das Unternehmen selbst richten und durch Unternehmensangehörige wiederkehrend in einer schematischen Form begangen werden. Die Begrenzung des sachlichen Anwendungsbereichs auf Unionsrecht gemäß Artikel 2 WBRL sollte im Rahmen des deutschen Umsetzungsgesetzes aufgehoben werden. Sinnvoll ist die Aufnahme von Straf- und Verbandstaten sowie die Einbeziehung sämtlicher Gesetze im materiellen Sinn. Zumal ein Hinweisgeber i.d.R. nicht beurteilen kann, ob ein Sachverhalt ein Verstoß gegen Unionsrecht darstellt und er somit Schutz genießt. Nach Artikel 18 WBRL sind alle eingehenden Meldungen zu dokumentieren. Nach Artikel 9 WBRL müssen die Meldekanäle so sicher konzipiert, eingerichtet und betrieben werden, dass die Vertraulichkeit der Identität des Hinweisgebers und Dritter, die in der Meldung erwähnt werden, gewahrt bleibt und nicht befugten Mitarbeitern der Zugriff darauf verwehrt wird. Alle Informationen, aus denen die Identität des Hinweisgebers direkt oder indirekt abgeleitet werden kann, unterliegen dem Vertraulichkeitsgebot gemäß Artikel 16 WBRL. Die Unabhängigkeit der Funktion von Personen oder Unternehmensabteilungen, die Meldungen entgegennehmen und Folgemaßnahmen ergreifen, muss gewährleistet sein.

Umgang mit anonymen Meldungen

Die WBRL stellt Vorgaben zur Einrichtung von Meldekanälen für die Entgegennahme anonymer Meldungen und zur Weiterverfolgung anonymer Meldungen in das freie Ermessen der nationalen Umsetzungsgesetzgeber. Ob potenzielle Whistleblower ohne die Implementierung anonymer Meldewege überhaupt bereit sein werden, Informationen weiterzugeben, wird entscheidend von der rechtlichen Ausgestaltung und praktischen Einhaltung des Vertraulichkeitsschutzes abhängen. Jedenfalls sollte es eine zwingende Pflicht zur Weiterverfolgung anonymer Meldungen geben. Es ist kein Grund erkennbar, warum eine anonyme Meldung nicht mit der gleichen Sorgfalt weiterverfolgt werden sollte wie eine vertrauliche oder offene Meldung, insbesondere wenn sie belastbare Information zu gravierenden Compliance-Verstößen enthält. In Deutschland entscheiden sich über die Hälfte der Whistleblower für eine anonyme Erstmeldung.[3]

3 vgl.: Colneric/Gerdemann a.a.O. S. 135 ff.

Vorrang interner Klärung

Grundsätzlich müssen sich Mitarbeiter mit Hinweisen zunächst an die vom Unternehmen vorgesehenen Ansprechpartner (etwa die Leitung des Compliancebereichs oder eine externe Ombudsperson) wenden. Für Unternehmen besteht die Möglichkeit, ein prämienbasiertes Hinweisgebersystem einzuführen. Der Hinweisgeber kann damit durch finanzielle Anreize zu internen Meldungen motiviert werden, bevor er sich an externe Stellen wie die Staatsanwaltschaft oder Presse wendet.[4] Eine interne Klärung kann dann unzumutbar sein, wenn die Geschäftsleitung an Straftaten beteiligt ist, diese duldet oder wenn es sich um besonders schwerwiegende Straftaten handelt. Nach Artikel 10 WBRL soll der Hinweisgeber in Zukunft auch bei direkter externer Meldung an die Behörden Schutz genießen. Unmittelbares öffentliches Whistleblowing wird nach Art. 15 Absatz 1 Buchst. b WBRL als schützenswert anerkannt, wenn der Whistleblower hinreichenden Grund zu der Annahme hat, dass der Verstoß eine unmittelbare oder offenkundige Gefährdung des öffentlichen Interesses

4 vgl.: Thomas Granetzny und Melena Krause: Was kostet ein gutes Gewissen? – Förderung von Whistleblowing durch Prämien nach US-Vorbild?, CCZ 2020, 29 ff.

darstellen kann, im Fall einer externen Meldung Repressalien zu befürchten sind oder aufgrund der besonderen Umstände des Falles geringe Aussichten bestehen, dass wirksam gegen den Verstoß vorgegangen wird. Enthüllungsplattformen wie Football Leaks oder anonyme Briefkästen führender Medienhäuser werden von Whistleblowern zunehmend genutzt. So waren die Panama Papers mit 2,6 Terabyte Daten das größte Leak, mit dem Journalisten je gearbeitet haben.

Pflicht zur Meldung

Es besteht grundsätzlich keine Verpflichtung des Arbeitnehmers, jegliches Fehlverhalten zu melden. Jedoch können gesetzliche oder arbeitsvertragliche Pflichten oder Obliegenheiten zur Abgabe von Hinweisen bestehen. Eine Hinweispflicht besteht jedenfalls dann, wenn ein Mitarbeiter konkreten Anlass zu der Annahme hat, dass ein bestimmter Sachverhalt eine Straftat darstellt, die dem Unternehmen oder Dritten schweren Schaden zuführen kann. Je schwerer der Regelverstoß wiegt, desto eher ist eine Meldung zumutbar. Je höher der Arbeitnehmer in der Hierarchieebene angesiedelt ist, desto eher muss er Compliance-Verstöße unabhängig von seiner Überwachungsaufgabe und Bezug zu seinem Aufgabenbereich melden. Die Mitbestimmungsrechte des Betriebsrats sind bei sind bei der Einführung und Ausgestaltung eines Whistleblowing-Systems zu beachten.

Gutgläubigkeit des Hinweisgebers

Hinweisgeber sollen nach Artikel 6 Absatz 1 WBRL dann geschützt sein, wenn sie zum Zeitpunkt der Meldung angesichts der Umstände und der verfügbaren Informationen hinreichenden Grund zu der Annahme haben, dass die von ihnen gemeldeten Sachverhalte der Wahrheit entsprechen. Diese Anforderung ist eine wichtige Schutzvorkehrung gegen böswillige oder missbräuchliche Meldungen, da sie gewährleistet, dass Personen keinen Schutz erhalten, wenn sie zum Zeitpunkt der Meldung willentlich und wissentlich falsche oder irreführende Informationen gemeldet haben. Gleichzeitig wird mit dieser Anforderung gewährleistet, dass der Schutz auch dann gilt, wenn ein Hinweisgeber in gutem Glauben ungenaue Informationen über Verstöße gemeldet hat. Aus welchen Gründen der Hinweisgeber Informationen meldet spielt keine Rolle.[5]

Schutz des Hinweisgebers vor Repressalien

Der Begriff der Repressalie ist nach Artikel 19 WBRL weit gefasst und schließt nicht nur Kündigungen ein. Erfasst sind beispielsweise auch Herabstufung oder Versagung einer Beförderung, Aufgabenverlagerung, Änderung des Arbeitsortes, Gehaltsminderung, Änderung der Arbeitszeit, Nötigung, Einschüchterung, Mobbing oder Ausgrenzung. Zugunsten des Whistleblowers ist nach Artikel 21 Absatz 5 WBRL die Einführung einer Beweislastumkehr vorgesehen.

Pflicht zur Durchführung interner Untersuchungen

Im Falle des begründeten Verdachts auf Compliance-Verstöße ist die Geschäftsleitung verpflichtet, eine interne Untersuchung durchzuführen.[6] Die Verdachtsschwelle hängt von der Plausibilität und Authentizität der Hinweise ab. Die Untersuchung erfolgt i. d. R. durch Wirtschaftsprüfer oder Rechtsanwälte als externe Ermittler und steht im Zusammenhang mit drohenden oder stattfindenden behördlichen Ermittlungen gegen das Unternehmen oder gegen Betriebsangehörige. Oberstes Ziel einer internen Untersuchung ist die umfassende Aufklärung des Sachverhalts. Zu ermitteln ist, welche Personen verwickelt sind. Die Compliance-Funktion des Unternehmens muss immer Zugang zu den Informationen der Hinweisgeber und der Untersuchung der externen Ermittler haben.[7] Bei fremdnützigen Compliance-Verstößen geht es um die Verhinderung weiterer Vermögensschäden, bei eigennützigen Compliance-Verstößen um die Reduzierung behördlicher Sanktionen. Für die betroffenen Personen gelten nach Artikel 22 WBRL die Wahrung der Unschuldsvermutung, die Verteidigungsrechte sowie das Recht auf Anhörung. Die Identität betroffener Personen bleibt während der Dauer einer Untersuchung geschützt.

Datenschutz-Richtlinie zum Hinweisgeberverfahren

Im Betrieb des Hinweisgebersystems sind die Richtlinien der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zu Hinweisgebersystemen zu beachten. Mit der Meldung von Verstößen gegen Verhaltenspflichten geht die Verarbeitung von personenbezogenen Daten einher. Betroffene Personengruppen sind vor allem die Hinweisgeber sowie die beschuldigten Personen. Es muss in jedem Einzelfall das konkrete Interesse des beschuldigten Arbeitnehmers an der Auskunftserteilung ermittelt und gegen das betriebliche Interesse des Arbeitgebers an der Auskunftsversagung beziehungsweise den berechtigten Interessen Dritter abgewogen werden.[8] Nach der WBRL sind die datenschutzrechtlichen Informationspflichten und Auskunftsrechte betroffener Personen wegen des Gebots der Vertraulichkeit der Identität des Whistleblowers einzuschränken. Als Voraussetzung einer Geltendmachung von Auskunftsrechten sollte der deutsche Umsetzungsgesetzgeber die objektive Unrichtigkeit der Meldung festlegen. Die Auskunft kann dann verweigert werden, wenn von der Gutgläubigkeit des Whistleblowers auszugehen ist.[9]

Meldekanal Compliance-Ombudsleute

Ombudsleute betreiben in der Funktion als vom Unternehmen bestellte Vertrauensanwälte einen externen Meldekanal für Hinweisgeber. Die Ombudsleute nehmen Hinweise auf mögliche Verletzungen von Gesetzen, internen Regelungen oder sonstigem schädigenden Verhalten entgegen und prüfen, ob die Hinweise plausibel und stichhaltig sind. In allen Compliance-relevanten Rechtsgebieten bereiten die Ombudsleute den Fall auf und geben eine rechtliche Einschätzung mit Handlungsempfehlungen für die Geschäftsleitung und die Compliance-Verantwortlichen.

5 vgl.: Colneric/Gerdemann a.a.O. S. 178
6 vgl.: Lambertus Fuhrmann: Internal Investigations: Was dürfen und müssen die Organe beim Verdacht von Compliance Verstößen tun?, NZG Heft 23/2016, S. 881 ff.; Cäcilie Lüneborg, Versicherbarkeit der Kosten Interner Untersuchungen, AG 23/2019, S. 863 ff.
7 vgl.: U.S. Department of Justice, Evaluation of Corporate Compliance Programs, Juni 2020
8 vgl.: Burkhard Fassbach und Frank Hülsberg: Beschäftigtendatenschutz im Hinweisgeberverfahren, GWR Heft 13 / 2020, S. 255 ff. m.w.N.
9 vgl.: Colneric/Gerdemann a.a.O. S. 177

Der Hinweisgeber entscheidet selbst, ob er dem Unternehmen gegenüber seine Identität wahren will oder nicht. Die Ombudsleute nehmen auch anonyme Hinweise entgegen.

Meldekanal Digitales Hinweisgebersystem

Internetbasierte Hinweisgebersysteme ermöglichen einen Dialog zwischen der Compliance Funktion und Hinweisgeber, ohne dass dieser seine Identität preisgeben muss. Hinweisgeber und Fallbearbeiter greifen von ihren jeweiligen Standorten auf den Server zu. Dabei wird lediglich der Inhalt der Meldungen gespeichert. Eine technische Rückverfolgung des Hinweises ist unmöglich. Der Hinweisgeber muss selbst darauf achten, dass er keine Informationen preisgibt, die Rückschlüsse auf seine Person zulassen. Die Befürchtung, unter dem Deckmantel der Anonymität nutzen Hinweisgeber den geschützten Kanal, um gezielt Kollegen in Misskredit zu bringen, kann durch wissenschaftliche Studien nicht belegt werden. Auch können solche Meldungen mit einer Plausibilitätsprüfung sehr gut herausgefiltert werden. Das digitale Hinweisgebersystem kann auch mit dem Institut der Ombudsperson als Meldekanal verbunden werden.

Compliance-Kommunikation

Das Unternehmen soll die Bereitstellung leicht zugänglicher und verständlicher Informationen über die Möglichkeit einer Meldung und das Hinweisgeberverfahren gewährleisten. Damit sollen Hinweisgeber eine fundierte Entscheidung darüber treffen können, ob, wann und auf welche Weise sie Meldung erstatten.[10] Mit einem zielführenden Kommunikationskonzept soll das Regelwerk der Unternehmensrichtlinie zum Hinweisgebersystem klar und verständlich kommuniziert werden. Erforderlich sind regelmäßige Compliance Schulungen sowie eine Rückkopplung an die Compliance Funktion, dass die Mitarbeiter die Inhalte auch verstanden haben. Whistleblowing ist zudem nur in einer wertebasierten

Unternehmenskultur sinnstiftend. Mitarbeiter müssen spüren und erleben, dass Compliance kein „Papiertiger" ist.

Fazit & Ausblick

Das Hinweisgebersystem ist ein unverzichtbares Element eines funktionierenden CMS. Um rechtliche Risiken frühzeitig zu identifizieren, implementieren immer mehr mittelständische Unternehmen solche Frühwarnsysteme. Best Practice sind digitale Plattformen und Compliance-Ombudsleute. Ein Whistleblowing-System muss klar und verständlich kommuniziert werden. Eine Unternehmensrichtlinie, Datenschutzrichtlinien sowie eine Betriebsvereinbarung müssen das Hinweisgeberverfahren rechtssicher und transparent abbilden. Schon heute gilt: Manager können wegen Verletzung von Organisations- und Aufsichtspflichten in Regress genommen werden, auch wenn sie persönlich an Compliance-Verstößen nicht beteiligt sind. Managerhaftungsfälle können am besten mit Compliance-Systemen vermieden werden. Der Whistleblower ist die Schlüsselfigur auf dem Compliance-Schachbrett. ■

10 vgl.: Erwägungsgrund 59 WBRL; ISO/DIS 37002 Whistleblowing Management Systems — Guidelines, 2020, 7.4 Communication

Dr. Burkhard Fassbach,
Rechtsanwalt,
Schneiders & Behrendt PartmbB

Dr. Frank Hülsberg,
Wirtschaftsprüfer,
Warth & Klein Grant Thornton AG

GVNW – immer gut informiert