DICO Arbeitspapier

A14 – Hinweisgeber- bzw. Whistleblowersysteme im Mittelstand

Autoren: Arbeitskreis Mittelstand I Stand: Oktober 2019

DICO
Deutsches Institut für Compliance

1. Warum ist die Einführung eines Hinweisgebersystems sinnvoll oder gar erforderlich?

Gesetzliche Regelungen zur Einrichtung von Hinweisgebersystemen existieren bereits für die sog. regulierten Sektoren wie die Branchen Banken und Versicherungen und Wertpapierhandel. Auch nach dem Geldwäschegesetz Verpflichtete oder an US-Börsen gelistete Unternehmen müssen Whistleblowersysteme einrichten.

Darüber hinaus empfehlen der Deutsche Corporate Governance Kodex (DCGK) und der ICC-Verhaltenskodex die Einrichtung von Hinweisgebersystemen.

Eine allgemeine, für alle Unternehmen geltende gesetzliche Verpflichtung zur Einrichtung gibt es damit zwar noch nicht, jedoch hat sich dies durch die im April 2019 im EU-Parlament vereinbarte EU-Richtlinie zum Schutz von Whistleblowern geändert. Nachdem die EU-Minister die Richtlinie am 07. Oktober 2019 verabschiedet haben, haben die EU-Mitgliedstaaten wie Deutschland zwei Jahre Zeit die Vorschriften in nationales Recht umzusetzen. Damit sind die folgenden Neuerungen verbunden:

- Verpflichtung aller Unternehmen ab 50 Beschäftigten zur Einführung eines Whistleblowersystems;
- dreigliedriges Meldesystem, bestehend aus:
  - internen Meldekanälen – vom Unternehmen bereitgestellt;
  - externen Meldekanälen – bspw. Strafverfolgungsbehörden, Gewerkschaften oder eigens eingerichteten Stellen;
  - öffentlichen Meldekanälen – bspw. Presse und sonstigen Medien;
- Whistleblower werden (gem. EU-Richtlinie) ermutigt, zunächst die internen vom Unternehmen einzurichtenden Meldekanäle zu benutzen;
- Frist zur Rückmeldung: Whistleblower sind innerhalb von drei Monaten (ab Meldungseingang) über Abhilfemaßnahmen zu informieren;
- Transparenz: Orientierungshilfe für Whistleblower erforderlich, ob, wann, wie und welche internen Meldekanäle genutzt werden können;
- Vertraulichkeit: Meldekanäle müssen so konzipiert sein, dass die Wahrung der Vertraulichkeit der Identität des Whistleblowers gewährleistet ist.

In dem Zusammenhang ist auch explizit auf das am 26. April 2019 in Kraft getretene Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) hinzuweisen. Der Ausnahmetatbestand des § 5 Nr. 2 GeschGehG normiert einen neuen weitreichenden Schutz von Hinweisgebern. So kann der Hinweisgeber Geschäftsgeheimnisse straffrei veröffentlichen soweit dies zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens erfolgt und die Erlangung, Nutzung und Offenlegung des Geschäftsgeheimnisses geeignet ist, das allgemeine öffentliche Interesse zu schützen.

Ungeachtet der rechtlichen Verpflichtungen gibt es für mittelständische Unternehmen weitere Gründe/Vorteile ein Hinweisgebersystem einzuführen:

- Schutz des Unternehmens, seiner Beschäftigten und seiner Organe;
- Früherkennung, Aufklärung und ggf. interne Sanktionierung von Regel- und Gesetzesverstößen innerhalb des kontrollierbaren Unternehmensumfeldes;
- unverzichtbarer Teil eines (zertifizierbaren bzw. prüfbaren) Compliance-Management-Systems und einer Vertrauenskultur im Unternehmen;
- Beitrag zur Minimierung von Reputations- und betriebswirtschaftlichen Schäden;
- Teil der positiven Außenwirkung und damit Wettbewerbsvorteil;
- Schutz von betroffenen Beschäftigten (bspw. Opfern von Diskriminierung);
- präventive Wirkung durch Abschreckungseffekt für potenzielle Täter;
- Erfüllung von Zertifizierungsanforderungen (bspw. IDW PS 980, ISO 19600);
- Beitrag zur Strafmilderung bzw. Exkulpation (Whistleblowersystem als wesentlicher Bestandteil eines Compliance-Management-Systems);
- Verhinderung von unternehmensschädlichen externen Meldungen an Behörden.

2. Welche Whistleblowersysteme kann ein Unternehmen zur Verfügung stellen? Und was sind die Vor- und Nachteile der einzelnen Meldekanäle?

1. Interne oder externe Systeme?

Hinweisgebersysteme können unterschiedlich ausgestaltet sein. Bei internen Hinweisgebersystemen werden die Meldungen gegenüber einer unternehmensinternen Stelle abgegeben. Hierbei kann es sich bspw. um den Compliance-Beauftragten oder die Interne Revision handeln. In jedem Fall sollte der eingebundene Personenkreis aus Vertraulichkeitsgründen stark begrenzt sein. Werden die Meldungen gegenüber einer vom Unternehmen benannten Hinweisgeberstelle außerhalb des Unternehmens abgegeben, spricht man von einem externen Hinweisgebersystem (nicht zu verwechseln mit dem in der EU-Richtlinie vorgesehenen externen Whistleblowing an Strafverfolgungsbehörden). Häufig handelt es sich hierbei um Rechtsanwälte oder andere Berufsträger in der Funktion als Ombudsperson, was jedoch nicht zwingend ist.

Vorteile internes Hinweisgebersystem	Vorteile externes Hinweisgebersystem
• Geringer Aufwand bei der Implementierung und keine Kosten für externe Stelle	• Gesetzliche Verschwiegenheitspflicht von Rechtsanwälten/Wirtschaftsprüfern
• Informationen landen „ohne Umwege“ direkt im Unternehmen	• Externe Ombudspersonen sind häufig erfahrene Compliance-Experten, die schnell eine valide rechtliche Ersteinschätzung abgeben können
• Interne Hinweisgeberstellen sind besser als externe mit internen Prozessen vertraut	• Keine potenzielle Beeinflussung der Hinweisgeberstelle durch Weisungsrechte von Vorgesetzten
• Vertrauensverhältnis der Mitarbeiter zur internen Stelle	• Manche Meldende bevorzugen den Kontakt zu einer externen Vertrauensperson.

Unternehmen können auch beide Varianten anbieten. Wichtig ist, dass die Hinweisgeberstellen über das erforderliche Know-how verfügen, die Relevanz von Hinweisen einzuschätzen und mit dem Hinweisgeber auf vertraulicher Ebene kommunizieren.

Das oberste Ziel bei der Implementierung von Hinweisgebersystemen wird dabei stets sein, potenzielle Verstöße zu identifizieren und die Abgabe von Hinweisen an Behörden, Presse oder sonstige Dritte (externe und öffentliche Meldekanäle) zu verhindern und den Hinweisgebern eine valide Alternative zur externen Meldung anzubieten.

2. Kommunikationskanäle

Das Hinweisgebersystem sollte bestenfalls verschiedene Kommunikationskanäle zur Verfügung stellen (E-Mail, Telefon und ggf. elektronische Kommunikationsplattformen). Elektronische Hinweisgebersysteme mit einem digitalen Meldekanal über eine web-basierte Kommunikationsplattform bieten folgende Vorteile:

> besonders gesicherte und anonyme Informationsübermittlung;

> Prozessdokumentation (Stichwort „Audit-Trail“);

> Möglichkeit zur vertraulichen (anonymen) Kommunikation zwischen Hinweisgeber und Annahmestelle (Stichwort „Chatkommunikation“);

> Plattformen für die Abwicklung von Fällen (Stichwort „Case Management“);

> die Produkte von etablierten externen Anbietern sind in der Regel erprobt;

> Möglichkeit der Arbeitserleichterung;

> Schaffung einer einheitlichen Lösung in unterschiedlichen Sprachen.

Die Preismodelle sind recht unterschiedlich. Es besteht die Möglichkeit, die elektronischen Hinweisgebersysteme sowohl mit internen als auch mit externen Hinweisgeberstellen (s. o. Ziff. 1) – einschließlich Ombudspersonen – zu kombinieren.

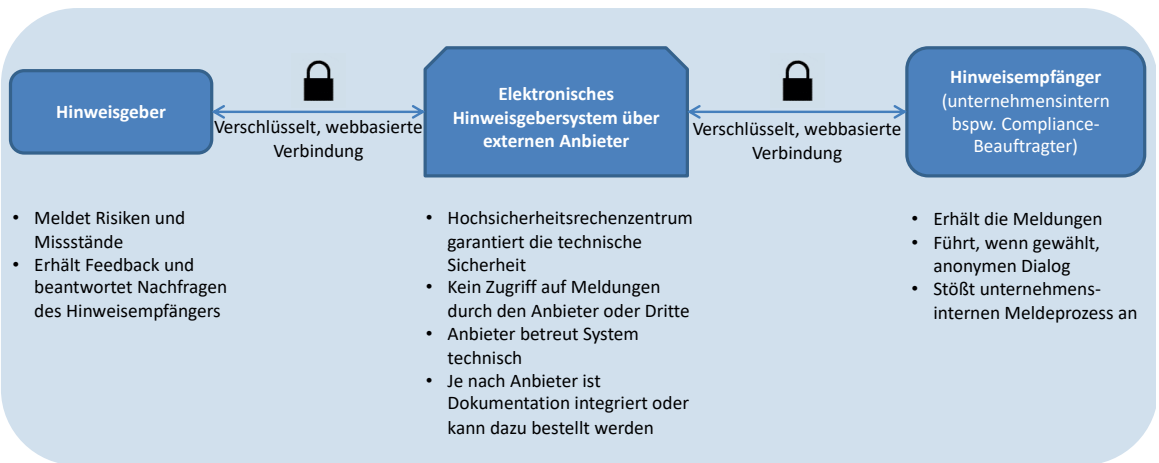

Abbildung 1: Elektronisches Hinweisgebersystem ohne Ombudsperson

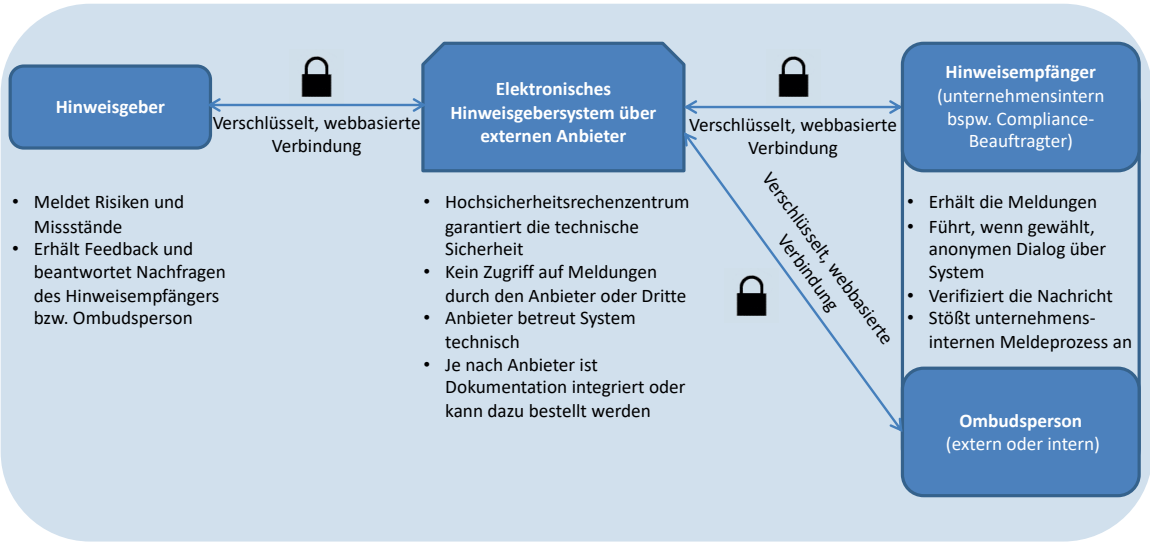

Abbildung 2: Elektronisches Hinweisgebersystem mit Ombudsperson

3. Definition der Prozesse

Für welches Modell sich Unternehmen auch entscheiden, die Prozesse sind klar zu dokumentieren und zu kommunizieren. Hierbei sind insbesondere folgende Punkte zu beachten:

> transparenter Prozess für Hinweisabgabe, Entgegennahme, Erstbewertung, Handlungsempfehlung, Benachrichtigung, Untersuchung, Reporting, Dokumentation und Löschung;

> Definition von Zuständigkeiten und Vier-Augen-Prinzip (bspw. Ombudsperson und Compliance-Beauftragter oder Compliance-Beauftragter und Revision);

> regelmäßige und effektive Kommunikation zur Nutzung von Hinweisgeberstellen gegenüber Beschäftigten. »

3. Was sind die Herausforderungen/Voraussetzungen?

Die Implementierung von Hinweisgebersystemen geht mit einigen Herausforderungen einher. Zudem müssen bestimmte Voraussetzungen erfüllt werden, um die Ziele eines solchen Systems erreichen zu können. Insbesondere datenschutz- und arbeitsrechtliche Vorgaben sind zu beachten.

1. Akzeptanz (Kultur):

Voraussetzung und Herausforderung zugleich ist es, eine hohe Akzeptanz für das Hinweisgebersystem zu erreichen. Hierfür ist es wichtig, dass die Kanäle nicht für missbräuchliche Meldungen genutzt werden. Allerdings sind nur wenige Meldungen als missbräuchlich einzustufen, was sich wiederum positiv auf die Akzeptanz auswirkt.

Maßgeblich beeinträchtigt wird die Akzeptanz weiterhin durch die folgenden Faktoren:

- Teilweise wird argumentiert, dass Hinweisgebersysteme mit Denunziation gleichzustellen sind. Es ist essentiell, die Personen mit Vorbehalten von der Vorteilhaftigkeit und Erforderlichkeit eines Hinweisgebersystems zu überzeugen.
- Die Akzeptanz für Hinweisgebersysteme ist leichter zu erlangen, wenn das Thema Compliance im Unternehmen bereits seit längerem einen hohen Stellenwert hat (Compliance-Kultur bereits stark etabliert).
- Redliche Hinweisgeber sind vor Repressalien zu schützen.
- Zu Unrecht beschuldigte Mitarbeiter sind vollständig zu rehabilitieren.

2. Kommunikation des Hinweisgebersystems:

Kommunikation ist ein weiteres Schlüsselelement für eine erfolgreiche Implementierung von Hinweisgebersystemen und die Anzahl der Meldungen. Dabei ist folgendes zu berücksichtigen:

- Das Hinweisgebersystem sollte bei Einführung transparent über verschiedene Kanäle kommuniziert werden (bspw. Intranet aber auch Internet, insbesondere wenn der Meldekanal auch für Unternehmensexterne geöffnet ist, schwarzes Brett, Videobotschaft der Geschäftsleitung, Schulung).
- Bei globalem Roll-Out des Hinweisgebersystems ist sicherzustellen, dass die Landesbesonderheiten berücksichtigt werden (auch: Kommunikation in Landessprache).
- Die Kommunikation ist fortlaufend zu wiederholen.

3. Involvierung anderer Abteilungen/Funktionen

Die Entscheidung für ein Hinweisgebersystem und dessen Ausgestaltung sollte nicht alleine durch die Unternehmensleitung und den Compliance-Beauftragten getroffen werden. Vielmehr sind andere Abteilungen und Funktionen ebenfalls mit einzubeziehen.

- Zu involvierende andere Abteilungen/Funktionen sind bspw. HR, Unternehmens-kommunikation, Datenschutz, IT, Arbeitnehmervertretung.
- Deren Involvierung erhöht die Akzeptanz und die Personen dienen als wichtige Multiplikatoren.
- Sie können entscheidende Hinweise geben bei der Auswahl des Meldekanals und den rechtlichen Anforderungen (bspw. Datenschutz und IT bei elektronischen Hinweisgebersystemen).

4. Anonymität und Vertraulichkeit

Verdachtsmomente werden eher gemeldet, wenn Anonymität und Vertraulichkeit gewahrt sind. Die Mitarbeiter sollten trotzdem ermutigt werden, ihre Identität preiszugeben. Dies erleichtert die Aufarbeitung des Verdachtsfalles.

- Anonymität und Vertraulichkeit sind nicht bei allen Hinweisgeberkanälen gewährleistet (bspw. E-Mail ohne Nutzung einer professionellen Kommunikationsplattform).
- Anonymität und Vertraulichkeit erhöhen die Akzeptanz und damit die Anzahl der zu erwartenden Meldungen.
- Die Möglichkeit, vertraulich melden zu können, sollte bei der Kommunikation hervorgehoben werden.

4. Fazit und Ausblick

Die Einrichtung eines Hinweisgebersystems sollte nicht nur als gesetzlich auferlegte Pflicht empfunden werden – der Mehrwert für das Unternehmen und seine Beschäftigten kann erheblich sein. Die Einrichtung eines auf die Bedürfnisse des Unternehmens zugeschnittenen Hinweisgebersystems empfiehlt sich. Es dient der Wahrung der Interessen des Unternehmens, Schaden von sich und seinen Mitarbeitern abzuwenden sowie Fehlentwicklungen und Missständen frühzeitig zu begegnen, und entspricht dem Bedürfnis des Hinweisgebers nach Schutz und Vertraulichkeit. »

Notizen

Notizen

Über DICO:

DICO – Deutsches Institut für Compliance e.V. wurde im November 2012 in Berlin auf Betreiben führender Compliance-Praktiker und -Experten gegründet und hat als gemeinnütziger Verein Mitglieder aus allen Branchen in Deutschland, darunter namhafte DAX-Unternehmen, Wirtschaftsprüfungs- und Beratungsgesellschaften sowie aus der Wissenschaft. DICO versteht sich als unabhängiges interdisziplinäres Netzwerk für den Austausch zwischen Wirtschaft, Wissenschaft, Politik und Verwaltung und sieht sich als zentrales Forum für die konsequente und praxisbezogene Förderung und Weiterentwicklung von Compliance in Deutschland.

DICO fördert Compliance in Deutschland, definiert in diesem Bereich Mindeststandards, begleitet Gesetzgebungsvorhaben und unterstützt zugleich die praktische Compliance-Arbeit in privaten und öffentlichen Unternehmen, fördert Aus- und Weiterbildung und entwickelt Qualitäts- sowie Verfahrensstandards.

DICO – Deutsches Institut für Compliance

Chausseestraße 13

D-10115 Berlin

info@dico-ev.de

www.dico-ev.de