

06.22

ZCG

Zeitschrift für
Corporate Governance

17. Jahrgang
Dezember 2022
Seiten 241 – 288

www.ZCGdigital.de

Leitung und Überwachung in der Unternehmens- und Prüfungspraxis

Fachbeirat:

Prof. Dr. Alexander Bassen,
Universität Hamburg

Prof. Dr. Dr. h. c. Theodor Baums,
Johann Wolfgang Goethe-Universität
Frankfurt am Main

Prof. Dr. Thomas Berndt,
Universität St. Gallen

WP/StB Prof. Dr. Manfred Bolin,
International School of Management,
Dortmund

Dr. Christine Bortenlänger,
Geschäftsführendes Vorstandsmitglied
Deutsches Aktieninstitut e.V.

Prof. Dr. Gerrit Brösel,
FernUniversität in Hagen

Prof. Dr. Henning Herzog,
QIRM Institut für Regulation &
Management e.G.

Ulrich Hocker, Hauptgeschäftsführer
Deutsche Schutzvereinigung für
Wertpapierbesitz e.V.

Prof. Dr. Anja Hucke, Universität Rostock

Prof. Dr. Annette G. Köhler,
Universität Duisburg-Essen

Prof. Dr. Stefan Müller, Helmut Schmidt
Universität Hamburg

Prof. Dr. Patrick Velte,
Leuphana Universität Lüneburg

Prof. Dr. Axel von Werder,
Technische Universität Berlin

WP/StB Prof. Dr. Norbert Winkeljohann,
Norbert Winkeljohann Advisory &
Investments

Prof. Dr. Henning Zülch,
Handelshochschule Leipzig (HHL)

ZCG

Management

Interne Untersuchungen in Deutschland 2022

[Ahrens/Michaelis, 245]

Interne Compliance- Maßnahmen bei Sanktionen

[Jungkind/Ludwig, 250]

ZCG

Recht

Das Hinweisgeberschutzgesetz

[Fissenewert, 254]

Aktuelle Rechtsprechung zur Corporate Governance

[Gebhardt, 260]

ZCG

Prüfung

Auswirkungen des Wirecard- Skandals
auf die Reputation des Abschlussprüfers

[Koch/Großeastroth, 265]

Vorstandsreporting und Kommunikation
mit dem Aufsichtsrat

[Adam/Labbé, 271]

ZCG

Rechnungs- legung

Empfehlungen zum sozialen Mindestschutz
in der Taxonomie-VO

[Baumüller, 279]

Das Hinweisgeber- schutzgesetz

Anmerkungen zum Gesetz und seiner Anwendung aus Governance-Sicht

Prof. Dr. Peter Fissenewert*

Der Bundestag hat am 29.9.2022 erstmals über einen Gesetzentwurf der Bundesregierung für einen besseren Schutz hinweisgebender Personen beraten. Am 19.10.2022 erfolgte eine öffentliche Anhörung im Rechtsausschuss. Der Gesetzentwurf der Bundesregierung will Hinweisgeberinnen und Hinweisgebern im beruflichen Umfeld künftig umfassender schützen. Für die Meldung von Verstößen im Unternehmen oder in einer Behörde sollen Meldestellen eingerichtet werden. Zudem sollen Hinweisgebende vor beruflichen Repressalien geschützt werden. Nach dem Gesetzentwurf müssen grundsätzlich alle Unternehmen mit mindestens 50 Mitarbeitenden eine interne Meldestelle einrichten, Unternehmen mit bis zu 249 Mitarbeiterinnen und Mitarbeitern können dabei Meldestellen gemeinsam aufbauen. Neben den internen Meldestellen sollen auch externe Meldestellen eingerichtet werden. Die hinweisgebende Person soll laut Entwurf wählen können, ob sie sich an eine interne oder eine externe Meldestelle wendet.

1. Grundlagen

1.1 Lob und Kritik

Das Gesetz ist längst überfällig – zum einen, weil die Europäische Richtlinie durch den deutschen Gesetzgeber bereits bis zum 17.12.2021 hätte umgesetzt werden müssen, zum anderen, um rechtliche Unsicherheiten zu beseitigen, etwa wann Hinweisgebende sich an Ermittlungsbehörden oder die Öffentlichkeit wenden dürfen und ob dies mit einer Kündigung „bestraft“ werden darf. Der Schutz durch das Gesetz soll jedoch nur bei Hinweisen auf Verstöße gegen bestimmte Rechtsnormen zur Geltung kommen, während zwar nicht strafwürdiges, aber unethisches Verhalten wie Vernachlässigungen in der Altenpflege nicht erfasst werden. Im Fall des Senders RBB wäre der bisher unbekannt Whistleblower, der den Skandal dort ins Rollen brachte, vom neuen Gesetz nicht

geschützt. Whistleblowers-Schutz im öffentlichen Dienst gibt es auch nicht für als Verschlussache deklarierte Dokumente. Edward Snowden wäre nach diesem Gesetz nicht geschützt.

1.2 Darum verdienen Hinweisgebende Schutz

In der Öffentlichkeit werden Whistleblower meist als Helden gefeiert. Edward Snowden oder Julian Assange, Wikileaks, Doping-Skandal, Panama-Papers, um nur wenige prominente Fälle zu nennen. Weniger spektakulär, aber wesentlich alltäglicher sind die vielen kleinen Fälle von Hinweisgebenden, die aber große Wirkung entfalten: Hinweisgebende in Unternehmen, Organisationen oder Behörden. Whistleblower gelten oft als Verräter. Sie werden von Arbeitgebern gestellt und ihnen wird gekündigt, zeigen zahlreiche

Fälle aus der Praxis. Zuverlässige Daten gibt es hierzu nicht.

Auch kleinere Enthüllungen sind wichtig, um darüber aufzuklären, was an Unregelmäßigkeiten passiert. Inge Hanne mann ist ein Beispiel dafür. Sie arbeitet seit 2005 im Jobcenter in Hamburg-Altona. Sie gilt als Hartz-4-Kritikerin und ihr Arbeitgeber warf ihr vor, dass Sie sich weigerte, bei Regelverstößen Sanktionen gegen Arbeitslose zu verhängen – ein Vorwurf, den sie bestreitet. Auf ihrem Blog kritisierte sie den Umgang mit Beziehenden von Arbeitslosengeld. Das gefiel dem Arbeitsamt nicht und so wurde sie mit sofortiger Wirkung vom Dienst freigestellt. Hannemann war die erste Mitarbeiterin eines deutschen Jobcenters, die sich öffentlich kritisch gegen die Arbeitsmarktpolitik der Agenda 2010 zu Wort meldete. Hartz 4 verfolge nicht das Ziel, Arbeitslosen eine Perspektive für den Wiedereintritt ins Leben zu bieten, sondern sie mittels Sanktionen aus dem Leistungsbezug zu drängen.

1.3 Whistleblowing als Teil der Compliance-Kultur

Risikomanagement und Kultur sind die wesentlichen Säulen eines funktionierenden Compliance-Management-Systems (CMS). Whistleblowing ist ein wesentliches Element für die Etablierung einer Compliance-Kultur im Unternehmen. Es ist nicht nur für die Mitarbeitenden eine Bereicherung, geschützt Hinweise geben zu können. Es ist auch eine Bereicherung für das Unternehmen. Schon bei der Implementierung entsprechender Systeme sollten die Mitarbeitenden darauf hingewiesen werden, dass Compliance alle angeht und die Erwartungshaltung besteht, dass jede Mitarbeiterin und jeder Mitarbeiter Fehlverhalten adressiert und sich nicht davon abwendet bzw. bewusst wegsieht. Damit wird Whistleblowing maßgeblich dazu beitragen, die Compliance-Kultur aufzubauen und zu stärken.

* Prof. Dr. Peter Fissenewert ist Rechtsanwalt und Partner der Kanzlei BUSE, Berlin.

► Statistisch gesehen ist die Gefahr der missbräuchlichen Nutzung kleiner als oft angenommen. ◀

1.4 Whistleblowing als Werkzeug zur Aufdeckung und Schadensabwehr und -begrenzung

Obwohl die Akzeptanz von CMS deutlich gestiegen ist, scheint die Anzahl von Compliance-Verfehlungen nicht zurückzugehen. Richtig ist aber auch, dass erst durch funktionierende CMS Verfehlungen aufgedeckt werden und entsprechende Meldemöglichkeiten (direkt und indirekt) erst durch CMS geschaffen wurden. Hierbei haben sich schon längst Hinweisgeberschutzsysteme (HGS) nach zahlreichen Studien als Hauptquelle für die Aufdeckung von Compliance-Verfahren herausgestellt.

Hinweise sind mit großem Abstand die häufigste Methode zur Aufdeckung von Compliance-Verstößen. So wurden 42 % der Compliance-Verstöße durch Hinweise aufgedeckt. Das sind fast dreimal so viele Fälle wie bei der nächsten Aufklärungsmethode, dem internen Audit mit einem Anteil von lediglich 16 % der Fälle.

Compliance-Verstöße, die durch aktive Methoden (wie eben HGS) aufgedeckt wurden, dauerten kürzer und führten im Durchschnitt zu geringeren Verlusten als solche, die passiv aufgedeckt wurden. Diese Daten verdeutlichen, dass proaktiv aufgedeckte Compliance-Verstöße i. d. R. zu geringeren Verlusten führen. Im Gegensatz dazu führt eine eher passive Aufdeckung zu länger andauernden Verstößen und damit einhergehend zu einem größeren finanziellen Schaden des Unternehmens.¹

Statistisch gesehen ist die Gefahr der missbräuchlichen Nutzung kleiner als oft angenommen. Erhebungen zeigen, dass nur jede zehnte Meldung verleumderisch ist.² Bei existierenden Meldesystemen, die viele Unternehmen bereits vor Inkrafttreten der EU-Richtlinie implementiert haben, kann bislang häufig per E-Mail, Briefkasten oder telefonisch Kontakt zu den verantwortlichen Stellen aufgenommen werden. Für diese Unternehmen ist mit der Einführung des neuen webbasierten Systems mit anonymer Meldeoption nicht mit einem schwunghaften Anstieg von Missbrauch zu rechnen.

Hinweisgeberschutz

2. Ausgestaltung des Hinweisgeberschutzsystems gem. HinSchG

2.1 HinSchG als Fundament

Mit der Frage, wie ein HGS erfolgreich implementiert werden kann, beschäftigen sich derzeit viele Unternehmen. Dabei ist die Motivation i. d. R. die neue gesetzliche Pflicht, weniger die Freiwilligkeit. Ein HGS kann eine wertvolle Informationsquelle zur Aufdeckung von rechtlichem Fehlverhalten sein. Je früher das Unternehmen davon erfährt, desto eher kann es sein Verhalten abstellen, das zu gravierenden Schäden führen könnte – ein Vorteil, der nicht selten verkannt wird.³

Das HinSchG bietet einige Vorgaben dazu, wie ein HGS auszusehen hat. Daneben finden sich Hinweise in der EU-Hinweisgeber-Richtlinie 2019/1937. Zusätzlich sind nationale Spezialgesetze bei der Implementierung zu beachten, etwa das nationale Arbeitsrecht und die Normen zum Datenschutzgesetz, insbesondere die Datenschutzgrundverordnung (DSGVO) und nationale Datenschutzgesetze. Bei international tätigen Unternehmen ist die Projektleitung auf Unterstützung aus den jeweiligen Ländern angewiesen. Dies kann weiteren zeitlichen und rechtlichen Prüfungsaufwand verursachen.

2.2 Wer ist geschützt?

Vom Gesetz geschützt sind:

- hinweisgebende Personen,
- Personen, die Gegenstand einer Meldung sind,
- sonstige Personen, die von einer Meldung betroffen werden.

Das Gesetz will nicht nur diejenigen Personen schützen, die Meldungen erstatten oder Verstöße offenlegen. Geschützt werden darüber hinaus auch Personen, die von der Meldung oder Offenlegung betroffen sind, etwa, indem sie dort genannt werden oder potenzielle Zeugen sein können. Nicht weniger wichtig ist dem Gesetzgeber, dass auch die Personen geschützt werden, die Gegenstand einer Meldung oder Offenlegung sind, d. h. denen in der Meldung oder Offenlegung ein Fehlverhalten vorgeworfen wird. Auch in Bezug auf diese Personen gilt es, die Vertraulichkeit der Identität zu schützen

und die geltenden Verfahrensrechte nicht zu beschränken. Daneben sollen auch die Rechte und Geheimhaltungsinteressen der von der Meldung und Offenlegung betroffenen juristischen Personen (insbesondere Unternehmen) geschützt werden. Nach allem ist also neben der eigentlichen Zielrichtung des HinSchG, den Schutz der hinweisgebenden Person zu verbessern, auch der Schutz dieser weiteren von der Meldung oder Offenlegung betroffenen Personen zu gewährleisten.

Der persönliche Anwendungsbereich ist weit gefasst. Ausdrücklich umfasst werden neben Arbeitnehmerinnen und Arbeitnehmern i. S. d. Art. 45 Abs. 1 AEUV einschließlich Beamtinnen und Beamten beispielsweise auch Selbstständige, Anteilseignerinnen und Anteilseigner, Mitarbeitende von Lieferanten und Personen, die bereits vor Beginn eines Arbeitsverhältnisses Kenntnisse von Verstößen erlangt haben.

2.3 Für welche Unternehmen gilt das Gesetz?

Das HinSchG bezeichnet Arbeitgeber, Unternehmen etc. als „Beschäftigungsgeber“.

Dies sind nach dem Gesetz (§ 3 Abs. 9 HinSchG):

- natürliche Personen sowie juristische Personen des öffentlichen und des privaten Rechts.
- rechtsfähige Personengesellschaften.
- sonstige rechtsfähige Personenvereinigungen, sofern mindestens eine Person bei ihnen beschäftigt ist.

Private Beschäftigungsgeber sind Beschäftigungsgeber mit Ausnahme juristischer Personen des öffentlichen Rechts und sol-

1 Vgl. <https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf> (Abruf: 3.11.2022), S. 21 f.

2 Vgl. Walter in Ruhmannseder/Behr/Krakow, Hinweisgebersysteme, 2021, S. 43

3 Vgl. Guttenberger, in: Ruhmannseder/Behr/Krakow, Hinweisgebersysteme, 2021, Rn. 99, 106; Moosmeyer, Compliance, 2021, Rn. 181; Roth, Compliance, 2020, S. 214/221; Drenckhahn, Checkliste: In fünf Schritten zum Hinweisgebersystem, CB 2021 S. 459

► Hinweisgebende Personen haben die Wahl, ob sie sich an eine interne oder externe Meldestelle wenden. ◀

cher Beschäftigungsgeber, die im Eigentum oder unter der Kontrolle einer juristischen Person des öffentlichen Rechts stehen.

2.4 Welche Unternehmen sind vom HinSchG erfasst?

Um ein weitgehendes und einheitliches Schutzniveau zu erreichen, wird der Kreis der Beschäftigungsgeber durch den Gesetzgeber weit gefasst. Dies sind:

- juristische Personen des Privatrechts wie Aktiengesellschaft, Kommanditgesellschaft auf Aktien, GmbH, Stiftung des Privatrechts, ebenso eingetragene Vereine und eingetragene Genossenschaften,
- juristische Personen des öffentlichen Rechts, insbesondere Gebietskörperschaften, Personalkörperschaften sowie Verbandskörperschaften auf Bundes- und Landesebene,
- rechtsfähige Personengesellschaften,
- sonstige rechtsfähige Personenvereinigungen.

Umfasst werden deshalb auch

- Anstalten, wie Landesrundfunkanstalten,
- öffentlich-rechtliche Stiftungen,
- evangelische und katholische Kirche mit ihren Kirchengemeinden,
- sonstige gem. Art. 140 GG, Art. 137 Abs. 5 WRV als Körperschaften des öffentlichen Rechts oder nach entsprechenden Bestimmungen des Landesrechts anerkannte oder als Vereine oder BGB konstituierte Kirchen und
- sonstige Religionsgemeinschaften.

2.5 Beweislastumkehr für Arbeitgeber

Repressalien und jedwede Vergeltungsmaßnahmen gegenüber Hinweisgebenden sind untersagt. In diesem Zusammenhang wird auch eine Regelung über eine Beweislastumkehr durch § 36 HinSchG eingeführt. Arbeitgeber müssen demnach künftig nachweisen, dass Maßnahmen gegen Arbeitnehmende nicht im Zusammenhang mit der Aufdeckung von Missständen stehen.

2.6 Loyalitäts- und Verschwiegenheitsklauseln sind nicht gültig

Es ist für ein Unternehmen nicht zulässig, sich auf die rechtlichen oder vertraglichen Pflichten des Einzelnen, beispielsweise Loyalitätsklauseln in Verträgen oder Vertraulichkeits- oder Geheimhaltungsvereinbarung zu berufen, um

- die Möglichkeit einer Meldung auszuschließen,
- Hinweisgebenden den Schutz zu versagen oder
- sie für die Meldung von Informationen über Verstöße oder einer Offenlegung mit Sanktionen zu belegen,

wenn die Weitergabe der Informationen, die unter diese Klauseln und Vereinbarungen fallen, notwendig ist, um den Verstoß aufzudecken.

2.7 Wahlmöglichkeit der Hinweisgebenden zwischen interner und externer Meldestelle

Hinweisgebende Personen haben die Wahl, ob sie sich an eine interne Meldestelle des Unternehmens oder eine externe Meldestelle, die durch Bund und Länder eingerichtet wird, wenden. Sie können somit den Meldekanal frei wählen, der sich angesichts der fallspezifischen Umstände für sie am besten eignet.

2.7.1 Externe Meldestelle

Eine zentrale externe Meldestelle soll beim Bundesamt für Justiz (BfJ) eingerichtet werden. Daneben sollen die bestehenden Meldesysteme bei der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und beim Bundeskartellamt als weitere externe Meldestelle mit Sonderzuständigkeiten weitergeführt werden. Die externe Meldestelle des Bundes beim BfJ soll mit einer Bund und Länder übergreifenden Zuständigkeit ausgestattet werden, die sowohl den öffentlichen Sektor als auch die Privatwirtschaft betrifft. Der externen Meldestelle des Bundes soll darüber hinaus die Aufgabe zukommen, Personen, die eine Meldung erwägen, umfassend über die zur Verfügung stehenden Verfahren zu informieren und zu beraten. Den Ländern steht es frei, für Meldungen, die die jeweilige Landesverwaltung und die je-

weiligen Kommunalverwaltungen betreffen, eigene externe Meldestellen einzurichten.

Die Aufgaben der externen Meldestelle sind mit denen der internen Meldestelle vergleichbar. Externe Meldestellen sind außerdem dazu verpflichtet, auf der Website umfangreiche Informationen über Abhilfemöglichkeiten und über den Hinweisgeberschutz bereitzustellen. Die externen Meldestellen arbeiten unabhängig und getrennt von den internen Meldestellen. Das Verfahren zur Bearbeitung einer externen Meldung ähnelt dem eines Verfahrens einer internen Meldung. Laut HinSchG hat die externe Meldestelle den Eingang einer Meldung umgehend zu bestätigen, spätestens nach sieben Tagen. Sie prüft die Stichhaltigkeit der Meldung und ergreift Folgemaßnahmen. Außerdem ist die externe Meldestelle dazu verpflichtet, der hinweisgebenden Person eine Rückmeldung nach spätestens drei Monaten zu erteilen.

2.7.2 Anonym oder öffentlich?

Nach dem HinSchG besteht keine direkte Verpflichtung, die Meldekanäle so zu gestalten, dass sie die Abgabe anonymer Meldungen ermöglichen. Vertraulichkeit und Anonymität gehen vor und dies ist ein klares Signal an die Mitarbeitenden.

Unternehmen sollen ein System implementieren, das die Vertraulichkeit von Hinweisen sicherstellt.⁴ Das System sollte darüber hinaus besondere Vorrichtungen für eine anonyme Abgabe von Hinweisen enthalten; ausnahmsweise und nur nach sorgfältiger Abwägung kann auf solche besonderen Vorrichtungen für die anonyme Abgabe von Hinweisen verzichtet werden. Die Vertraulichkeit kann im Grundsatz auch durch den Einsatz von Ombudspersonen gewährleistet werden, die zur vertraulichen Behandlung der Identität des Hinweisgebenden auch gegenüber dem Auftraggeber vertraglich verpflichtet werden. Die Stellung von Ombudspersonen gegenüber Ermittlungsbehörden ist allerdings – etwa in Bezug auf

⁴ Vgl. Rudkowski/Schreiber, Aufklärung von Compliance-Verstößen, 2015, S. 191; Kaetzler, in: Zentes/Glaab, GWG – Geldwäschegesetz, 2022, GWG, § 6, Rn. 161.

► Unternehmen mit bis zu 249 Beschäftigten können mit anderen Unternehmen zusammen eine gemeinsame Meldestelle betreiben. ◀

den Beschlagnahmenschutz – rechtlich nicht völlig gesichert.⁵ Auch der Datenschutz bietet hier bisweilen Grenzen des Vertrauens- und Identitätsschutzes, etwa wenn ein vom Hinweisgebenden genannter Arbeitnehmender Auskunftsrechte gegenüber dem Unternehmen geltend macht.⁶

2.7.3 Intern besser als extern

Insgesamt ist davon auszugehen, dass es im ureigensten Interesse eines Unternehmens sein sollte, dass sich die hinweisgebende Person an die eigene interne Meldestelle wendet und nicht an eine externe Meldestelle. Nur so erlangt man die Hoheit des Verfahrens und kann soweit erforderlich zügig schadensbegrenzende Maßnahmen einleiten. Eine hinweisgebende Person wird sich aber nur dann an eine interne Meldestelle wenden, wenn sie darauf vertrauen kann, dass die Meldung ernst genommen und unter Beachtung der Vertraulichkeit bearbeitet wird, dass Maßnahmen ergriffen werden und dass keine Repressalien zu erwarten sind. Ein integriertes Topmanagement und eine professionelle interne Kommunikation zum Thema Hinweisgeber sind unverzichtbare Voraussetzungen für den Aufbau dieser Vertrauenskultur.

2.8 Anforderungen an die interne Meldestelle

Nach § 12 HinSchG müssen alle Unternehmen mit mehr als 50 Mitarbeitenden eine eigene interne Meldestelle einrichten. Gem. § 16 HinSchG sind die Meldekanäle so zu gestalten, dass nur die für die Entgegennahme und Bearbeitung der Meldungen zuständigen sowie die sie bei der Erfüllung dieser Aufgaben unterstützenden Personen Zugriff auf die eingehenden Meldungen haben. Es muss also sichergestellt werden, dass keine unberechtigten Personen Zugriff auf die Identität der hinweisgebenden Person oder den Hinweis selbst haben. Dies hat zugleich Auswirkungen auf die technische Ausgestaltung des internen Meldekanals.

Interne Meldekanäle müssen Meldungen in mündlicher oder in Textform ermöglichen. Mündliche Meldungen müssen per Telefon oder mittels einer anderen Art der

Hinweisgeberschutz

Sprachübermittlung möglich sein. Auf Ersuchen der hinweisgebenden Person ist für eine Meldung innerhalb einer angemessenen Zeit eine persönliche Zusammenkunft mit einer für die Entgegennahme einer Meldung zuständigen Person der internen Meldestelle zu ermöglichen.

Von besonderer Bedeutung ist dabei der Schutz der Vertraulichkeit der Identität der hinweisgebenden Person. Wesentlich für die Akzeptanz des Hinweisgeberverfahrens ist ein wirksamer Schutz der Identität der hinweisgebenden und aller von einer Meldung betroffenen Personen. Die Identität darf dabei grundsätzlich nur den jeweils für die Bearbeitung einer Meldung zuständigen Personen bekannt sein. Informationen über die Identität einer hinweisgebenden Person oder einer Person, die Gegenstand einer Meldung ist, sollen nur in Ausnahmefällen herausgegeben werden dürfen, etwa in Strafverfahren oder auf Verlangen der Strafverfolgungsbehörden.

Unternehmen mit bis zu 249 Beschäftigten können mit anderen Unternehmen zusammen eine gemeinsame Meldestelle betreiben. Wer keine interne Meldestelle einrichtet oder keine interne Meldestelle betreibt, kann mit einer Geldbuße bis zu 20.000 Euro belegt werden.

2.9 Welche Meldekanäle kommen für Unternehmen in Frage?

Auf diese Frage gibt es keine pauschale Antwort. Eine geeignete Lösung hängt u. a. von der Branche und der jeweiligen Größe des Unternehmens ab. Ebenso sollten das rechtliche Umfeld und die Struktur sowie das zur Verfügung stehende Budget bei einer Entscheidung mit einbezogen werden.

Die bislang bekannten Meldekanäle sind in Bezug auf ihre Praxistauglichkeit sehr unterschiedlich zu bewerten. Außerdem kann auch der kombinierte Einsatz mehrerer Kanäle erwogen werden. Unternehmen berichten, dass hierdurch die Zahl der Meldungen steigt. Mitarbeiter loben im Gegenzug, dass ihre Motivation und Bedürfnisse durch eine Auswahl zwischen Meldekanälen besser zum Zuge kommen. Schon allein das Zurverfügungstellen ei-

nes Hinweisgeberkanals wird von Mitarbeitern belohnt.

Ein HGS ist mehr als ein Briefkasten und auch mehr als eine Hotline. Das simpelste Tool für ein HGS ist ein ganz normaler Briefkasten. Tatsächlich sollten eine Hotline, ein Weblink, die Kontaktadresse und weitere Möglichkeiten, die auf den ersten Blick nach einem „Briefkasten für Meldungen“ aussehen, mehr als das sein.

2.10 Digitales HGS

Die Etablierung eines digitalen Meldesystems ermöglicht es Unternehmen, den gesetzlichen Anforderungen für die Einrichtung eines internen Meldekanals vollumfänglich gerecht zu werden, Risiken frühzeitig zu identifizieren und Reputationssschäden ebenso wie Haftungsrisiken zu vermeiden.

Ein digitales Meldesystem lässt sich außerdem optimal in ein bestehendes CMS integrieren, ist zu jeder Uhrzeit und von jedem Ort aus erreichbar und bietet der hinweisgebenden Person eine zentrale Anlaufstelle.

2.11 Wer darf Hinweise entgegennehmen?

Nach § 15 HinSchG müssen die mit den Aufgaben einer internen Meldestelle beauftragten Personen bei der Ausübung ihrer Tätigkeit unabhängig sein. Sie können neben ihrer Tätigkeit für die interne Meldestelle andere Aufgaben und Pflichten wahrnehmen. Es ist dabei allerdings sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu Interessenkonflikten führen.

3. Welche Rechtsgebiete werden vom Hinweisgeberschutz umfasst?

Hinweisgebende Personen sollen auf den Schutz des HinSchG vertrauen können, wenn sie Fehlverhalten melden. Dabei

⁵ LG Bochum v. 16.3.2016 – II 6 Qs 1/16 sowie Rudolf, StraFo 2019 S. 57 ff.; DICO Standard 11, S. 9.

⁶ LAG Baden-Württemberg v. 20.12.2018 – 17 Sa 11/18, Rn. 207 (juris); Altenbach/Dierkes, EU-Whistleblowing-Richtlinie und DSGVO, CCZ 2020 S. 126.

kann das Fehlverhalten auf das Unternehmen zurückzuführen sein, weil es vielleicht hiervon profitiert. Umgekehrt kann aber auch das Fehlverhalten in einer Schädigung des Unternehmens selbst liegen.

Einige Beispiele:

- ▶ Lebensmittel werden umetikettiert, um höherwertig bzw. noch haltbar zu sein.
- ▶ Das Unternehmen unterlässt die vorgeschriebenen Qualitätskontrollen.
- ▶ Der Vertrieb besticht mit Wissen der Geschäftsführung Kunden, um wichtige Aufträge zu erhalten.
- ▶ Es werden Preis- oder Gebietsabsprachen getroffen, um den Wettbewerbsdruck zu mildern.
- ▶ Das Unternehmen publiziert geschönte Zahlen.
- ▶ Ein Beratungsunternehmen stellt dem Kunden mehr Stunden in Rechnung als wirklich angefallen sind.
- ▶ Ein Automobilhersteller verzichtet aus Kostengründen auf eine erforderliche Rückrufaktion zum Austausch sicherheitsrelevanter defekter Teile.
- ▶ Ein Vertriebsmitarbeiter in der Versicherungsbranche fälscht Kundenverträge, um eine höhere Vertriebsprovision zu bekommen.
- ▶ Mitarbeiter fälschen Anwesenheits- und Urlaubslisten, um eine höhere Vergütung zu bekommen.
- ▶ Mitarbeiter nutzen den Dienstwagen ohne Genehmigung für private Zwecke.
- ▶ Mitarbeiter stehlen Waren eines Kaufhauses.

Das HinSchG nennt ausdrücklich folgende Vorschriften:

- a) Verstöße gegen Strafvorschriften: Dies umfasst jede Strafnorm nach deutschem Recht.
- b) Verstöße, die bußgeldbewährt sind, soweit die verletzte Vorschrift dem Schutz von Leben, Leib und Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient: Diese Regelung ist nach dem Willen des Gesetzgebers weit zu verstehen. Eine Bußgeldvorschrift dient dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der

Rechte von Beschäftigten oder ihrer Vertretungsorgane, wenn sie diesen Schutz bezweckt oder dazu beiträgt, den Schutz der genannten Rechtsgüter und Rechte zu gewährleisten. Darunter fallen beispielsweise Vorschriften aus folgenden Bereichen:

- ▷ Arbeitsschutz
- ▷ Gesundheitsschutz
- ▷ Verstöße gegen das Mindestlohngesetz
- ▷ Vorgaben des Arbeitnehmerüberlassungsgesetzes
- ▷ Bußgeldvorschriften, die Verstöße gegen Aufklärungs- und Auskunftspflichten gegenüber Organen der Betriebsverfassung (z. B. Betriebsräte, Gesamtbetriebsräte, Konzernbetriebsräte, Wirtschaftsausschüsse) sanktionieren (§ 121 Betriebsverfassungsgesetz)

c) Darüber hinaus sind alle Verstöße gegen Rechtsnormen umfasst, die zur Umsetzung europäischer Regelungen getroffen werden. Dies umfasst viele Bereiche, die zur Umsetzung der EU-Whistleblower-Richtlinie im HinSchG enthalten sind, darunter die folgenden:

- ▷ Regelungen zur Bekämpfung der Geldwäsche
- ▷ Vorgaben zur Produktsicherheit
- ▷ Vorgaben zur Beförderung gefährlicher Güter
- ▷ Vorgaben zum Umweltschutz und Strahlenschutz
- ▷ Lebensmittel- und Futtermittelsicherheit
- ▷ Qualitäts- und Sicherheitsstandards bei Arzneimitteln und Medizinprodukten
- ▷ Regelungen des Verbraucherschutzes
- ▷ Regelungen des Datenschutzes
- ▷ Sicherheit in der Informationstechnik
- ▷ Vergaberecht
- ▷ Regelungen zur Rechnungslegung bei Kapitalgesellschaften

4. Praxishinweise

Unternehmen können ebenso entscheiden, dass auch über das CMS hinausgehende Sachverhalte bzw. über das HinSchG

▶ Bei Sanktionierung einer juristischen Person oder Personenvereinigung beträgt die maximale Geldbuße für die Nicht-Wahrung der Vertraulichkeit eine Million Euro. ◀

hinausgehende Sachverhalte mitgeteilt werden können, beispielsweise erhebliche Reputationsrisiken, soweit dafür keine sonstigen Kanäle eingerichtet werden.⁷

4.1 Meldestellen

Meldestellen können insbesondere:

- ▶ interne Untersuchungen durchführen und betroffene Personen und Arbeitseinheiten kontaktieren,
- ▶ die hinweisgebende Person an andere zuständige Stellen verweisen,
- ▶ das Verfahren aus Mangel an Beweisen oder aus anderen Gründen abschließen,
- ▶ das Verfahren an eine zuständige Behörde zwecks weiterer Untersuchungen abgeben.

Das HinSchG regelt auch die Folgen eines nicht gesetzeskonformen Verhaltens. In § 40 HinSchG finden sich die entsprechenden Bußgeldvorschriften.

4.2 Bußgelder

Bußgelder werden fällig für

- ▶ die wissentliche Offenlegung einer unrichtigen Information,
- ▶ die Nicht-Einrichtung und das Nicht-Betreiben einer internen Meldestelle,
- ▶ die Behinderung einer Meldung oder den Versuch einer Behinderung,
- ▶ eine Repressalie oder den Versuch einer Repressalie gegen hinweisgebende Personen,
- ▶ die vorsätzliche oder fahrlässige Nicht-Wahrung der Vertraulichkeit.

Die Geldbußen können je nach Fall bis zu 100.000 Euro betragen. Bei Sanktionierung einer juristischen Person oder Personenvereinigung beträgt die maximale Geldbuße für die Nicht-Wahrung der Vertraulichkeit eine Million Euro.

4.3 Einführung eines Hinweisgeber-systems

Egal, ob freiwillig oder durch gesetzliche Pflicht: Mit der Umsetzung des Hinweis-

⁷ Vgl. Thüsing/Forst, in: Thüsing, Beschäftigten-datenschutz und Compliance, 2021, Kap. 6, Rn. 25 ff.; Inderst/Steiner, in: Inderst/Bannenberg/Poppe, Compliance, 2017, Kap. 3, Rn. 61; DICO Standard 11, S. 9

► Der Aufbau auf Basis eines PDCA-Modells ist auch dafür hilfreich, das System später zertifizieren zu lassen. ◀

gebersystems sollte alsbald begonnen werden. Unabhängig davon, ob man gleich nach einem ISO-Standard vorgehen will oder erst später: wenn überhaupt, bietet sich hier die Plan-Do-Check-Act-Methode (PDCA) an.

4.4 Implementierung nach dem PDCA-Modell

PDCA (Plan-Do-Check-Act), also Planen, Umsetzen, Prüfen, Handeln, ist eine Methode, um Teamprozesse und Produkte kontinuierlich zu verbessern. Der PDCA-Zyklus ist ein Modell zur Umsetzung von Veränderungen. Die Management-Normen der ISO (z. B. ISO 9001 für Qualitätsmanagement oder ISO 37002 für CMS) basieren auf dieser Methode. Wer ein ISO-Management-System kennt, findet sich auch in den anderen Systemen leicht zu recht. Nach dem PDCA-Zyklus soll ein System oder eine Maßnahme zunächst geplant (Plan) werden, anschließend wird sie umgesetzt (Do), dann ihre Wirksamkeit evaluiert (Check), damit sie anschließend bei Bedarf angepasst werden kann (Act).

PDCA ist eine einfache Methode, mit der Teams wiederkehrende Fehler vermeiden und Prozesse verbessern können. In der

Planungsphase ist schlicht zu planen, was zu tun ist. Abhängig vom Umfang des Projekts kann die Planung einen großen Teil der Arbeit des Teams beanspruchen. Normalerweise besteht der Prozess aus kleineren Schritten, sodass ein ordentlicher Plan mit weniger Fehleranfälligkeit erarbeitet werden kann.

Die Umsetzungsphase bedeutet, den Plan in eine Handlungsphase zu überführen. In dieser Phase ist alles umzusetzen, was in der vorherigen Phase berücksichtigt wurde.

In der Prüfungsphase ist die Umsetzung des Plans zu prüfen und auch, ob der ursprüngliche Plan tatsächlich funktioniert hat. Darüber hinaus kann das Team problematische Teile des aktuellen Prozesses identifizieren und für die Zukunft beseitigen bzw. verbessern. Wenn während des Prozesses etwas schiefgelaufen ist, sollte es analysiert und die Ursache der Probleme gefunden werden.

Die Handlungsphase stellt die letzte Phase des Zyklus dar. Zuvor wurde der Plan entwickelt, umgesetzt und überprüft. Jetzt muss auf die Ergebnisse reagiert werden.

Im Ergebnis bietet PDCA wesentliche Vorteile:

- Förderung der kontinuierlichen Verbesserung von Menschen und Prozessen,
- Teamerfahrung, mögliche Lösungen in einem kleinen Maßstab und in einer kontrollierten Umgebung zu testen,
- Verhinderung, dass wiederkehrende Fehler den Arbeitsprozess stören

Der Aufbau auf Basis eines PDCA-Modells ist auch dafür hilfreich, das System später zertifizieren zu lassen. Der neue Standard für ein CMS, der ISO 37301, stärkt auch den Schutz von Hinweisgebern. Diese Norm ist zertifizierbar.

Auch für die Einrichtung von HGS gibt es einen ISO-Standard: den ISO 37002. Er zielt darauf ab, Richtlinien für die Implementierung, Verwaltung, Evaluierung, Aufrechterhaltung und Verbesserung von effektiven Hinweisgebern bereitzustellen. Derzeit ist ISO 37002 aber (noch) nicht zertifizierbar.

In jedem Fall sollten die Implementierungen, gleich welcher Art und gleich nach welchem Ziel, dem PDCA-Standard folgen, um später darauf eine Zertifizierung aufbauen zu können.