Hochschule Hof
University of Applied Sciences

Hofer akademische Schriften

zum Recht in Nachhaltigkeit, Compliance und IT

Herausgegeben von Prof. Dr. Beatrix Weber

Band 2

Sarah Ciasto

Die Umsetzung des Hinweisgeberschutzgesetzes in Unternehmen

Eine Betrachtung aus der Risikoperspektive unter Anwendung einer Balanced Score Card

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der deutschen Nationalbibliografie;detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Hofer akademische Schriften zum Recht in Nachhaltigkeit, Compliance und IT
Herausgegeben von Prof. Dr. Beatrix Weber
Professorin für Gewerblichen Rechtssschutz und IT-Recht an der Hochschule Hof / University of Applied Sciences

Band 2

Sarah Ciasto

Die Umsetzung des Hinweisgeberschutzgesetzes in Unternehmen – Eine Betrachtung aus der Risikoperspektive unter Anwendung einer Balanced Score Card

Der vorliegende Text wurde ursprünglich im Sommersemester 2023 als Masterarbeit an der Hochschule für angewandte Wissenschaften Hof, Studienfakultät für Weiterbildung, Studiengang Master Compliance, IT und Datenschutz, eingereicht und betreut durch Prof. Dr. Beatrix Weber, Professorin für Rechtssschutz und IT-Recht

Druck und Verlag:
Hochschule Hof, Studienfakultät für Weiterbildung, Alfons-Goppel-Platz 1, D-95028 Hof

ISBN: 978-3-935565-30-1
https://doi.org/10.57944/1051-143

Abstract

Die Umsetzungsfrist der Richtlinie (EU) 2019/1937 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (Whistleblower-Richtlinie) ist in Deutschland zum 17.12.2021 erfolglos abgelaufen. Ein vom Bundestag verabschiedeter Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz) hat am 10. Februar 2023 im Bundesrat keine Mehrheit erhalten. Mit einem zeitnahen Abschluss des Gesetzgebungsverfahrens ist dennoch zu rechnen, da die Koalition das Gesetzesvorhaben nun in zwei Teile gefasst hat, welche seit dem 14. März 2023 in das parlamentarische Verfahren eingebracht wurden.

Die Umsetzung des Hinweisgeberschutzgesetzes in Unternehmen birgt an einigen Stellen rechtliche Unsicherheiten, woraus Risiken resultieren können. So geht die vorliegende Arbeit der Frage nach, ob eine Balanced Score Card für Unternehmen im Umgang mit rechtlichen Unsicherheiten und aus der Umsetzung des Hinweisgeberschutzgesetzes resultierenden Risiken eine geeignete Hilfestellung darstellen könnte.

Um die Forschungsfrage zu beantworten, wurde zunächst die Eignung einer Balanced Score Card als Instrument des Risikomanagements untersucht. Anschließend wurden rechtliche Unsicherheiten und Risiken, welche für Unternehmen durch die Umsetzung des Hinweisgeberschutzgesetzes entstehen könnten, herausgearbeitet. Behandelt wurden dabei die Themengebiete persönlicher und sachlicher Anwendungsbereich, Anreize zur Wahl der internen Meldestelle, zentrale Konzernmeldestelle, anonyme Meldungen, Schutzvoraussetzungen, Repressalienverbot und Beweislastumkehr sowie interne Untersuchungen als Folgemaßnahmen. Im Anschluss wurde eine Risiko-Balanced Score Card für den Umgang mit dem Hinweisgeberschutzgesetz erstellt und das Vorgehen geprüft und bewertet. Zuletzt wurden Handlungsempfehlungen für Unternehmen herausgearbeitet.

Die Risiko-Balanced Score Card kann als Instrument zur Risikoidentifikation und -analyse und als Grundlage für die Risikobewertung dienen. Für viele Unternehmen kann sie als Hilfestellung im Umgang mit den genannten Risiken gelten, da für sie eine Pflicht zur Einrichtung interner Meldekanäle besteht und daraus Schutzansprüche für Whistleblower entstehen können.

Die Umsetzung des Hinweisgeberschutzgesetzes in Unternehmen

Eine Betrachtung aus der Risikoperspektive unter Anwendung einer Balanced Score Card

MASTERARBEIT

zur Erlangung des Grades Master of Laws (LL. M.)

an der Hochschule für Angewandte Wissenschaften Hof
Studiengang Compliance, IT und Datenschutz

---

vorgelegt von:

Sarah Ciasto
Paarangerweg 4
86415 Mering

---

vorgelegt bei:

Erstprüferin:
Prof. Dr. Beatrix Weber
Alfons-Goppel-Platz 1
95028 Hof

Zweitprüfer:
Prof. Dr. Gerald Schmola
Alfons-Goppel-Platz 1
95028 Hof

Mering, 05. April 2023

Inhaltsverzeichnis

Abkürzungsverzeichnis

a. A.	andere Ansicht
Abs.	Absatz
Abschn.	Abschnitt
AcP	Archiv für die civillistische Praxis
Art.	Artikel
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AktG	Aktiengesetz
ArbRAkt	Arbeitsrecht Aktuell
ARP	Arbeitsschutz in Recht und Praxis
AZ	Aktenzeichen
BAG	Bundesarbeitsgericht
BB	Betriebsberater
BeckRS	Beck-Rechtsprechung
BetrVG	Betriebsverfassungsgesetz
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
bspw.	beispielsweise
BSC	Balanced Score Card
BT-Drs.	Drucksache des deutschen Bundestages
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
CB	Compliance Berater
CCZ	Corporate Compliance Zeitschrift
CMS	Compliance Management System
DB	Der Betrieb
DSGVO	Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung)
DStR	Deutsches Steuerrecht
EGMR	Europäischer Gerichtshof für Menschenrechte
ErwG	Erwägungsgrund
ErfK	Erfurter Kommentar zum Arbeitsrecht
ESG	Zeitschrift für nachhaltige Unternehmensführung
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuZA	Europäische Zeitschrift für Arbeitsrecht
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
f. / ff.	folgende/fortfolgende
FH	Formulierungshilfe
gem.	gemäß
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
ggf.	gegebenenfalls
HinSchG	Gesetz für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz), Beschlussempfehlung und Bericht des Rechtsausschusses v. 14.03.2023, BT-Drs. 20/5992
HinSchG-RefE	Referentenentwurf des Bundesministeriums der Justiz zum HinSchG v. 13.04.2022

Hrsg.	Herausgeber
HSI	Hugo Sinzheimer Institut für Arbeits- und Sozialrecht
IDW	Institut der Wirtschaftsprüfer
i. S. d.	im Sinne des/der
ISO	International Organization für Standardization
i. V. m.	in Verbindung mit
KSchG	Kündigungsschutzgesetz
KWG	Kreditwesengesetz
lit.	littera/Buchstabe
LkSG	Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten
NJOZ	Neue Juristische Online-Zeitschrift
Nr.	Nummer
NZA	Neue Zeitschrift für Arbeitsrecht
NZG	Neue Zeitschrift für Gesellschaftsrecht
NZWiSt	Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht
OLG	Oberlandesgericht
OWiG	Gesetz über Ordnungswidrigkeiten
PS	Prüfungsstandard
RdA	Recht der Arbeit
RFamU	Recht der Familienunternehmen
Rn.	Randnummer
Rz.	Randziffer
S.	Seite
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
U.	Urteil
Urt. v.	Urteil vom
v.	vom
VAG	Versicherungsaufsichtsgesetz
VerSanG	Gesetz zur Stärkung der Integrität in der Wirtschaft
Vgl.	Vergleiche
Vol.	Volume
WBRL	Richtlinie (EU) 2019/1937 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden
WpHG	Wertpapierhandelsgesetz
z. B.	zum Beispiel
ZCG	Zeitung für Corporate Governance
ZRFC	Risk, Fraud & Compliance
ZRP	Zeitschrift für Rechtspolitik

Darstellungsverzeichnis

Einführung

Die Frist zur nationalen Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (Richtlinie EU 2019/1937) verstrich bereits am 17. Dezember 2021. Der am 16. Dezember 2022 vom Bundestag verabschiedete Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz) hat am 10. Februar 2023 im Bundesrat keine Mehrheit erhalten. Da wesentliche Teile des Gesetzes nicht der Zustimmung des Bundesrates bedürfen, hat die Koalition das Gesetzesvorhaben nun in zwei Teile gefasst, wovon nur noch einer zustimmungsbedürftig ist. Beide Entwürfe vom 14. März 2023 werden nun in das parlamentarische Verfahren eingebracht.[1]

Die Umsetzung des HinSchG in Unternehmen birgt an einigen Stellen rechtliche Unsicherheiten, woraus Risiken resultieren können. *So geht die vorliegende Arbeit der Frage nach, ob eine Balanced Score Card (BSC) für Unternehmen im Umgang mit rechtlichen Unsicherheiten und aus der Umsetzung des Hinweisgeberschutzgesetzes resultierenden Risiken eine geeignete Hilfestellung darstellen könnte.*

Dafür wird zunächst die Eignung der BSC als Instrument des Risikomanagements untersucht. Dabei wird auf den Zusammenhang zwischen Compliance und Risiko, den Risikobegriff und die Risikoarten sowie die Übertragung der BSC in das Risikomanagement eingegangen. Anschließend werden rechtliche Unsicherheiten und Risiken, welche für Unternehmen durch die Umsetzung des HinSchG entstehen könnten, herausgearbeitet. Behandelt werden hier die Themengebiete persönlicher und sachlicher Anwendungsbereich, Anreize zur Wahl der internen Meldestelle, zentrale Konzernmeldestelle, anonyme Meldungen, Schutzvoraussetzungen, Repressalienverbot und Beweislastumkehr sowie interne Untersuchungen als Folgemaßnahmen. Anschließend wird eine Risiko-BSC für den Umgang mit dem HinSchG erstellt und das Vorgehen geprüft und bewertet. Abschließend werden Handlungsempfehlungen für Unternehmen erläutert und die Ergebnisse zusammenfassend dargestellt. Berücksichtigt wurde der Stand des Gesetzgebungsverfahrens bis einschließlich 04. April 2023.

[1] Vgl. Bundesregierung, 2023, Online-Artikel.

A. Balanced Score Card als Instrument des Risikomanagements

Die Einführung neuer Gesetze wie dem HinSchG birgt Unsicherheiten und Risiken für Unternehmen. Zunächst wird untersucht, inwieweit Methoden des Risikomanagements im Compliance-Umfeld Anwendung finden können. Insbesondere wird darauf eingegangen, ob sich eine Balanced Score Card als Instrument im Umgang mit Risiken anbietet. Zunächst wird dafür der Zusammenhang zwischen Compliance und Risiko erklärt, anschließend der Risikobegriff sowie die verschiedenen Risikoarten erläutert. Danach werden die Grundlagen des Risikomanagements dargestellt sowie die Eignung der BSC als Instrument des Risikomanagements herausgearbeitet.

I. Compliance und Risiko

Unter *Compliance* versteht man als Bestandteil einer Good Corporate Governance die Einhaltung, Befolgung und Übereinstimmung mit Recht und Gesetz, organisationsinternen Normen sowie ethischen Richtlinien und Werten.[2] Sie dient der Vermeidung von Haftung und Strafen für das Unternehmen, seine Organe und Mitarbeiter; umstritten ist aber seit langem ob eine Rechtspflicht zu Compliance besteht.[3] Für Unternehmen aus den Bereichen der Bank-, Finanz- und Versicherungsdienstleistungen besteht eine ausdrückliche gesetzliche Regelung gem. § 2 a KWG, § 33 WpHG und § 64 a VAG. Für sonstige Unternehmen und Organisationen wird eine Pflicht zu Compliance aus §§ 76 Abs. 1, 91 Abs. 2, 93 AktG und § 43 GmbHG abgeleitet. So sind gem. § 91 Abs. 2 AktG geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden können. Compliance ist dabei eine *Matrixaufgabe*, die sich über die gesamte Organisation erstreckt, siehe Abbildung 1.[4]

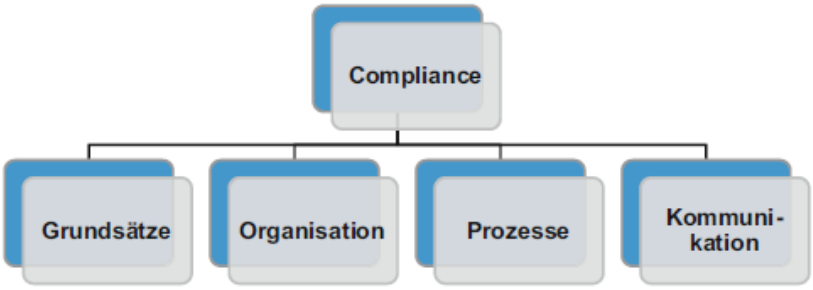


Abbildung 1: Compliance als Matrixaufgabe[5]

[2] Vgl. Behringer, 2018, S. 36; Romeike, 2018, S. 15f; Weber, 2016, S. 4f; Vetter, 2013, S. 3f.
[3] Vgl. Behringer, 2018, S. 37f; Weber, 2016, S. 10; Vetter, 2013, S. 4ff.
[4] Vgl. Weber, 2016, S. 12; Withus, 2014, S. 3.
[5] Vgl. Weber, 2016, S. 12.

Die *Compliance Grundsätze* leiten sich aus internen Regelungen wie Arbeits- und Tarifverträgen, Betriebsordnungen, Richtlinien, Code of Conduct oder Verpflichtungserklärungen sowie externen Regelungen wie Rechtsnormen, Best Practice Regelungen oder Selbstverpflichtungen ab. Die *Compliance Organisation* umfasst die Verantwortlichkeiten der Unternehmensleitung, die Möglichkeit der Delegation an Arbeitnehmer und die Eingliederung in die Aufbauorganisation eines Unternehmens. Daneben sollte Compliance auch in *Unternehmensprozesse*, also die Ablauforganisation, integriert werden. Dazu gehören Prinzipien wie Vieraugenprinzip, Kontrolle und Dokumentation, Transparenz sowie regelmäßige Berichterstattung. Ein weiteres entscheidendes Element ist die *Compliance Kommunikation*. Hier sollte durch proaktive Kommunikationsmaßnahmen Vertrauen, Transparenz und Nachvollziehbarkeit von Regelungen geschaffen werden.[6]

Ein *CMS* sollte in jedem Fall ein Teil des Risikomanagements eines Unternehmens sein.[7] Dies entspricht auch dem Ansatz des integrierten Risikomanagements. So sollte eine ganzheitliche Betrachtung der Corporate Governance – also der Bereiche Risikomanagement, integriertes Kontrollsystem, Compliance und Revision – erfolgen.[8] Geschehen kann dies durch integrierte Methoden, Systeme und Prozesse. Vorteile dieses Ansatzes sind Kostenvorteile in der Generierung von Informationen, Transparenz und eine Vielzahl von Möglichkeiten zur Steigerung der Effektivität und Effizienz. Der Aufbau eines CMS sollte dem Dreiklang von Konzeption, Implementierung und Kontrolle nachkommen.[9] Bei der Konzeption werden Rechtsrahmen und Risiken erfasst und in Prozesse sowie die Organisation überführt. Implementierung bedeutet Umsetzung der Prozesse und Schulung der Mitarbeitenden. In regelmäßigen Abständen sollten im Rahmen einer Kontrolle Selbst- oder Fremd-Auditierungen vorgenommen werden. Neben einer anlassbezogenen oder reaktiven Prüfung sollte Compliance präventiv interne Regularien, Prozesse, Organisation und Kontrollen umfassen.[10]

Ein CMS kann anhand verschiedener *Standards* wie dem IDW PS 980 oder der ISO 37301geprüft und zertifiziert werden. Näher eingegangen wird an

[6] Vgl. Weber, 2016, 12ff.
[7] Vgl. Hauschka, 2016, Rn. 8; Weber, 2016, S. 12; Withus, 2014, S. 115; Wengert/Schittenhelm, 2013, S. 8.
[8] Vgl. Otremba, 2019, S. 1; Romeike, 2018, S. 15f; Tüllner, 2012, S. 118.
[9] Vgl. Weber, 2016, S. 12.
[10] Vgl. Weber, 2016, S. 6.

dieser Stelle auf den Umgang dieser beiden Standards mit *Compliance-Risiken*. Diese stellen gem. *IDW PS 980*[11] ein Grundelement des CMS dar. Die Feststellung und Beurteilung von Compliance-Risiken ist die Grundlage für die Entwicklung eines angemessenen CMS. Dies kann durch die systematische Aufnahme der Risiken für Regelverstöße erfolgen, bspw. in Form von Interviews, Workshops oder der Auswertung von verfügbaren Informationen anderer Unternehmen. Die grundsätzlichen Entscheidungen der gesetzlichen Vertreter zur Risikosteuerung (Risikovermeidung, -reduktion, -überwälzung, -akzeptanz) sollten bei der Risikoanalyse berücksichtigt werden. Das Befassen mit Compliance-Risiken ist ein Regelprozess, der einen wesentlichen Bestandteil der kontinuierlichen Weiterentwicklung und Verbesserung des CMS eines Unternehmens darstellt. Auch gem. *ISO 37301*[12] soll die Organisation auf der Grundlage einer Compliance-Risikobeurteilung ihre Risiken identifizieren, analysieren und bewerten. Diese müssen zum einen regelmäßig überprüft werden und zum anderen sobald wesentliche Veränderungen der Umstände oder des Kontextes der Organisation auftreten. Charakterisiert werden können Compliance-Risiken durch Grundursachen und Quellen sowie Folgen der Nichtbeachtung und Wahrscheinlichkeit des Auftretens der Konsequenzen. Als beispielhafte Konsequenzen werden Personen- und Umweltschäden, wirtschaftliche Verluste, Beschädigung des Ansehens sowie administrative, zivilrechtliche und strafrechtliche Haftung genannt. Explizit erwähnt wird, dass geschätzte finanzielle Konsequenzen der Non-Compliance auf keinen Fall mit der Wahrscheinlichkeit des Auftretens multipliziert werden sollten, da dies das Szenario des ungünstigsten Falles herausrechnet und üblicherweise zu ungeeigneten Risikobehandlungsmaßnahmen führt. Umfang und Detailgrad der Compliance-Risikobeurteilung sind von Risikosituation, Kontext, Größe und Zielen der Organisation abhängig und können für spezifische Teilbereiche eines Unternehmens variieren.

Die Identifizierung und Bewertung des *relevanten Rechtsrahmens* sowie möglicher Änderungen und die Bewertung der Nicht-Einhaltung von rechtlichen Vorgaben ist eine der Aufgaben von Compliance.[13] Einer der im

[11] Vgl. IDW PS 980, 2011, S. 22, A16.
[12] Vgl. DIN ISO 37301, S. 17, 20, 39f.
[13] Vgl. Weber, 2016, S. 4.

IDW PS 980 beispielhaft genannten relevanten Faktoren für die Risikoanalyse sind Änderungen im rechtlichen Umfeld, die ISO 37301 nennt Veränderungen der Compliance-Verpflichtungen als Grund für eine (neue) Risikobeurteilung.[14] Die mit der Umsetzung des neuen HinSchG einhergehenden Risikobewertung fällt somit in den Aufgabenbereich von Compliance.
Da ein CMS im Wesentlichen so aufgebaut ist wie ein Risikomanagementsystem[15], ist die *Anwendung von Methoden des Risikomanagements* in diesem Zusammenhang durchaus sinnvoll. Weiter nennen die beiden Standards IDW PS 980 und ISO 37301 in ihren Ausführungen zu den Compliance-Risiken Begriffe aus dem Risikomanagement. Beispiele hierfür sind die systematische Aufnahme von Risiken, die Entscheidungen zur Risikosteuerung, der Dreiklang aus Identifikation, Analyse und Bewertung sowie das Herausarbeiten der Ursachen und Folgen sowie die Wahrscheinlichkeit des Auftretens von Konsequenzen. Nachfolgend werden der Risikobegriff und die verschiedenen Risikoarten erläutert.

II. Risikobegriff und -arten

In der *Rechtswissenschaft* findet man auf nationaler, europäischer und internationaler Ebene unterschiedliche Legaldefinitionen des *Risikobegriffs*; überwiegend wird Risiko hier aber als Produkt von Eintrittswahrscheinlichkeit und Folgenschwere bzw. Höhe des drohenden Schadensereignisses definiert.[16] Besondere Anforderungen an das Recht im Umgang mit Risiken stellt die Wissenschaftsbezogenheit.[17] Sie ist eine verfahrensrechtliche Komponente zur angemessenen Risikoabschätzung und -bewertung; dies bedeutet, dass die zum aktuellen Stand vorhandenen Erkenntnisquellen ausgeschöpft werden sollen, bevor Entscheidungen auf ungewisser Grundlage getroffen werden. Es müssen Verfahren vorgesehen werden, durch die notwendiges Wissen generiert und dem jeweiligen Entscheidungsträger zur Kenntnis gebracht wird. Das Wissen muss in eine für den Entscheidungsträger verwertbare Form gebracht werden, indem Handlungsoptionen und damit verbundene Chancen, Risiken und Ungewissheiten offengelegt werden.[18]

[14] Vgl. DIN ISO 37301, S. 40; IDW PS 980, S. 22, A16.
[15] Vgl. Henschel/Heinsche, 2016, S. 182; Wengert/Schittenhelm, 2013, S. 8.
[16] Vgl. Klafki, 2017, S. 10f, 383.
[17] Vgl. Klafki, 2017, S. 24ff.
[18] Vgl. BVerfGE 50, 290, 334; Klafki, 2017, S. 24f; Wahl/Appel, 1995, S. 126.

Nach dem Verständnis des *Risikomanagements* beschreibt der Begriff Risiko eine potenziell negative, unerwünschte und ungeplante Abweichung von den Zielsystemen.[19] Risiken sind also Ereignisse und mögliche Entwicklungen innerhalb einer Organisation, welche sich negativ auf die Erreichung der Unternehmensziele auswirken. Je nach Informationsgrundlage können Risiken in drei Risikotypen eingeteilt werden: unbekannte Risiken, bekannte/nicht bewertete Risiken und bekannte/gesteuerte Risiken.[20] Innerhalb des Risikomanagements erfolgt die quantitative Bewertung von Risiken durch potenzielle Schäden oder Schadenszenarien und den damit verknüpften Häufigkeiten bzw. Eintrittswahrscheinlichkeiten.[21] Ziel des Risikomanagements ist die Vermeidung von Schäden und Nachteilen für ein Unternehmen.[22]

Da *Compliance* wie bereits erläutert ein Teil des Risikomanagements ist, gilt hier das gleiche Verständnis des Risikobegriffs. Risiken im Compliance-Bereich sind Gefahren und werden als Ursache von Schäden durch die Verletzung von vorgegebenen Regeln aufgefasst.[23] Auch können Compliance-Risiken entstehen, wenn sich zu beachtende Regeln verändern oder neue zu beachtende Regeln auftreten.[24] Besonders ist bei der Risikobetrachtung im Compliance-Bereich, dass sich die Risiken sehr wenig für eine mathematische Berechnung eignen, wodurch es ausreichend ist die Risiken in verschiedene Wahrscheinlichkeitsgruppen (bspw. sehr unwahrscheinlich, möglich, wahrscheinlich, sehr wahrscheinlich) einzuteilen.[25]

Da unternehmerisches Handeln ohne das Eingehen von Risiken nicht möglich ist, stehen Organisationen vielfältigen Risiken gegenüber.[26] Zunächst werden die dem Risikomanagement bekannten *Risikoarten* aufgezählt: Risiken des Geschäftsbetriebs, Personalrisiken, führungsbezogene Risiken, leistungsbezogene Risiken, finanzielle Risiken, Marktpreisrisiken, Kontrahentenrisiken, Risiken bezüglich der allgemeinen Sicherheit, Arbeitsschutzrisiken, Marktrisiken, Technologierisiken, Rohstoffrisiken, Risiken aus dem gesetzlichen Rahmen, Umweltrisiken, naturbezogene Risiken und politische Risiken.[27]

[19] Vgl. Romeike, 2018, S. 8ff; Brühwiler, 2001, S. 8.
[20] Vgl. Romeike, 2018, S. 10.
[21] Vgl. Romeike, 2018, S. 36.
[22] Vgl. Schmola, 2016, S. 289.
[23] Vgl. Gleißner, 2020, S. 24.
[24] Vgl. Withus, 2014, S. 131.
[25] Vgl. Withus, 2014, S. 125.
[26] Vgl. Schmola, 2016, S. 300.
[27] Vgl. Schmola, 2016, S. 300ff; Withus, 2014, S. 42; Dillerup, 2013, S. 886; Wengert/Schittenhelm, 2013, S. 27ff.

Auf die für den Compliance-Bereich relevanten Risiken wird nun genauer eingegangen.[28] Strategische Compliance-Risiken gefährden Organisationen als Ganzes, Beispiele hierfür sind Reputations- und Imageschäden aufgrund von Rechtsverstößen sowie Schadensrisiken bei Vermögens- oder Bilanzdelikten. Regulatorische Risiken entstehen insbesondere bei Änderungen des rechtlichen Umfelds. Operative Risiken liegen in der Gestaltung der organisationsinternen Prozesse entlang der Wertschöpfungskette. Finanzielle Compliance-Risiken umfassen die Schadensfolgen von Verstößen, Sanktionen und Bußgelder sowie den Verlust von Geschäft als indirekte Folge von Compliance-Verstößen und Imageschäden. Personal-Risiken ergeben sich aus strafrechtlich relevantem Verhalten von Unternehmensangehörigen wie bspw. Korruption oder Betriebsspionage. Rechtswidriges Verhalten zivilrechtlicher Art oder mit Bußgeld bedrohtes Handeln, Verstöße gegen interne Richtlinien und damit einhergehenden Nebenpflichten aus dem Arbeitsvertrag sowie gegen kulturelle und soziale Regeln gehören ebenfalls dieser Kategorie an.

Anschließend werden die Grundlagen des Risikomanagements erläutert und die Anwendbarkeit einer BSC im Umgang mit Risiken geprüft.

III. Risikomanagement

Das *Risikomanagement* beschäftigt sich als Teil der Corporate Governance[29] mit der systematischen Abwehr bzw. Minimierung von Risiken und umfasst sämtliche Maßnahmen zur planmäßigen zielgerichteten Analyse, Beeinflussung und Kontrolle von Risiken.[30] Es ist darauf ausgerichtet, kritische Situationen im Rahmen der Unternehmenstätigkeiten frühzeitig zu erkennen, zu vermeiden oder zu reduzieren bzw. die Wirkung der Risiken zu minimieren.[31] Risikomanagement konzentriert sich auf Entscheidungen unter Risiko sowie Entscheidungen unter Unsicherheit.[32] Bei Entscheidungen unter Unsicherheit sind mögliche Szenarien und Auswirkungen nicht oder nicht vollständig bekannt, wodurch keine Eintrittswahr-

[28] Vgl. Pauthner/Stephan, 2016, Rn. 31; Weber, 2016, S. 5f.
[29] Vgl. Dillerup, 2013, S. 883.
[30] Vgl. Romeike, 2018, S. 16; Pampel/Krolak, 2016, Rn. 39; Schmola, 2016, S. 289, 303.
[31] Vgl. Brauweiler, 2019, S. 1; Romeike, 2018, S. 9.
[32] Vgl. Romeike, 2018, S. 12.

scheinlichkeiten angegeben werden können. Bei Entscheidungen unter Risiko dagegen sind Informationen über die möglichen Alternativen als auch ihre Eintrittswahrscheinlichkeiten vorhanden.

Der *Risikomanagementprozess* zeigt in Abbildung 2 die nötigen Schritte, die für die Umsetzung des Risikomanagements notwendig sind.

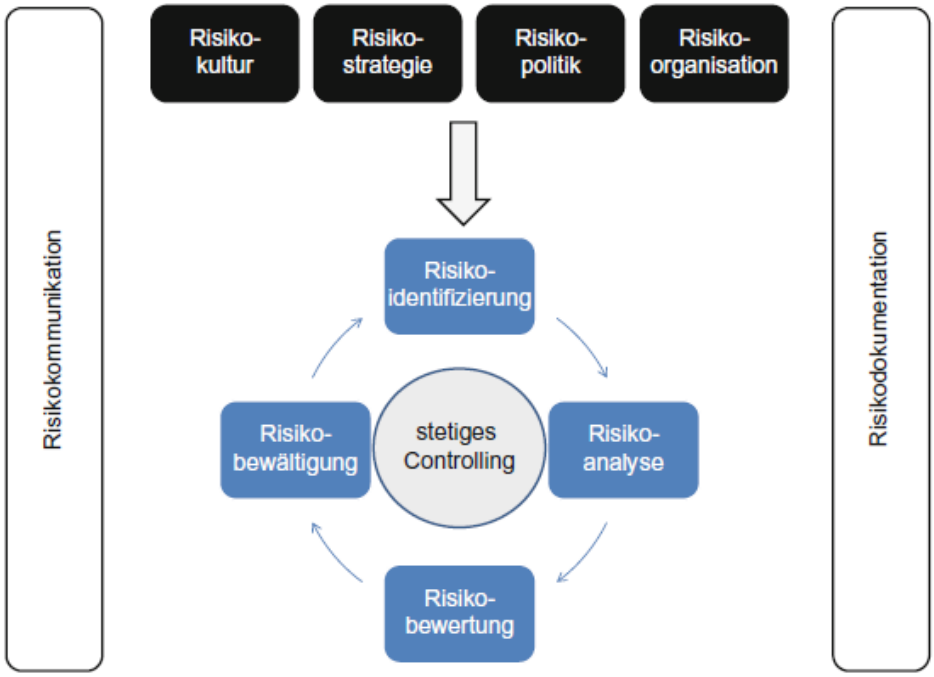


Abbildung 2: Risikomanagementprozess[33]

Als Basis des Risikomanagements dienen Risikostrategie, -kultur, -politik -organisation, -kommunikation und -dokumentation.[34] Anschließend folgen im Rahmen des operativen Risikomanagementprozesses Risikoidentifizierung, -analyse, -bewertung und -bewältigung.[35] Um den Gefahren vorzubeugen oder ihre Auswirkungen abzuschwächen, werden im Anschluss im Rahmen der Risikobewältigung Maßnahmen abgeleitet.[36]

Auf die einzelnen *Inhalte des Risikomanagementprozesses* aus Abbildung 2 wird nun detaillierter eingegangen. Die Rahmenbedingungen für das Risikomanagement werden durch die *Risikostrategie* vorgegeben. Diese beschreibt durch Leitlinien den Umgang mit Risiken, wobei sie auf

[33] Vgl. Schmola, 2016, S. 304.
[34] Vgl. Romeike, 2018, S. 36; Schmola, 2016, S. 304.
[35] Vgl. Glage/Grötzner, 2016, Rn. 56ff; Pampel/Krolak, 2016, Rn. 41; Schmola, 2016, S. 304.
[36] Vgl. Schmola, 2016, S. 303, 306.

Art der Risiken, Risikotoleranz, Herkunft der Risiken, Zeithorizont der Risiken und die Risikotragfähigkeit eingeht.[37] Konkretisiert wird die Risikostrategie durch die *Risikopolitik*, welche die Grundzüge zur Analyse, Bewertung und Bewältigung einzelner Risiken festlegt.[38] Die *Risikokultur* entsteht aus dem Unternehmen selbst heraus durch Unterstützung und unter Vorbildfunktion der Leitung und beschreibt als Teil der Unternehmensstruktur das Verhalten der Mitarbeiter im Umgang mit Risiken.[39] Die Arbeitnehmenden sollen durch die *Risikokommunikation* über die festgelegte Risikopolitik, die Risikostrategie und die identifizierten Risiken sowie die geplanten Maßnahmen informiert und für das Risikomanagement sensibilisiert werden.[40] Die *Risikoorganisation* umfasst neben der Ernennung eines Risikomanagers den Aufbau eines Risikomanagementteams sowie die Ernennung eines Lenkungsteams.[41] Dokumente und Aufzeichnungen sollten im Rahmen der *Risikodokumentation* ebenso festgehalten werden wie Risikopolitik, Prozesse, Formulare und Checklisten.[42]

Auf den *operativen Risikomanagementprozess* – also die Risikoidentifizierung, -analyse, -bewertung und -bewältigung – wird an dieser Stelle vertiefter eingegangen. Seine Darstellung als Kreislauf ist sinnvoll, weil die stetige Wiederholung und Überwachung der Phase notwendig ist, da sich bestehende Risiken jederzeit verändern, wegfallen oder neue Risiken hinzukommen können.[43] Die eingeleiteten Maßnahmen sollten somit stetig durch das *Risikocontrolling* hinsichtlich ihrer Wirksamkeit kontrolliert werden, wodurch der Risikomanagementprozess neu startet und dabei auf eine kontinuierliche Verbesserung ausgerichtet ist.[44]

Die *Risikoidentifizierung* ist die systematische und kontinuierliche Erfassung der auf das Unternehmen einwirkenden Unsicherheiten.[45] Für ein qualitatives Ergebnis sollen hier Risikoquellen, betroffene Bereiche, Ereignisse und Entwicklungen berücksichtigt werden.[46] Der Erfolg des Risikomanagements ist maßgeblich von einer effektiven Risikoerkennung bzw.

[37] Vgl. Romeike, 2018, S. 36; Glage/Grötzner, 2016, Rn. 48f; Schmola, 2016, S. 305.
[38] Vgl. Löber, 2015, S. 21.
[39] Vgl. Schmola, 2016, S. 304.
[40] Vgl. Schmola, 2016, S. 310.
[41] Vgl. Glage/Grötzner, 2016, Rn. 51ff; Schmola, 2016, S. 305f.
[42] Vgl. Schmola, 2016, S. 310f.
[43] Vgl. Schmola, 2016, S. 306.
[44] Vgl. Glage/Grötzner, 2016, Rn.57; Schmola, 2016, S. 310.
[45] Vgl. Dillerup, 2013, S. 886.
[46] Vgl. Romeike, 2018, S. 36.

Informationsbeschaffung abhängig, da nicht erkannte Risiken nicht weiter analysiert und bearbeitet werden können.[47] Mögliche Instrumente der Risikoidentifizierung sind bspw. Brainstorming, Workshops, Interviews, Besichtigungen, Checklisten, strategische Analysen, Szenario-Analysen, Schadensfallanalysen und -statistiken, Bilanzen, Organisationspläne, Risikoaudits oder Fehler-Möglichkeits- und Einflussanalysen.[48] Das Ergebnis der Risikoidentifizierung ist ein Risikoinventar oder -portfolio.[49]

Ziel der *Risikoanalyse* ist es, ein Verständnis für die Risiken zu entwickeln sowie ihre Ursachen, Wirkungszusammenhänge, Auswirkungen und Häufigkeit bzw. Wahrscheinlichkeit ihres Eintretens zu erkennen.[50] Risiken werden also durch die Bestimmung ihrer potenziellen Auswirkungen analysiert – dies kann je nach Risiko, Zweck und den verfügbaren Informationen, Daten und Ressourcen mit verschiedener Untersuchungstiefe durchgeführt werden.[51]

Durch die *Risikobewertung* wird das Ausmaß der identifizierten Risiken ermittelt, wobei Eintrittswahrscheinlichkeit und Schadensausmaß eine wichtige Rolle spielen.[52] Gemessen werden können diese beiden Werte qualitativ oder quantitativ.[53] Eine mögliche qualitative Kategorisierung der Auswirkungen könnte von unbedeutend bis katastrophal erfolgen, die Eintrittswahrscheinlichkeit von sehr unwahrscheinlich bis sehr wahrscheinlich.[54] Als qualitatives Maß können beispielsweise statistische Eintrittswahrscheinlichkeiten oder das mögliche Gewinn- oder Verlustpotenzial einer Entwicklung dienen.[55] Auch Erfahrungswerte, Branchenvergleiche, Studien oder Einschätzungen von Fachexperten können Angaben liefern.[56]

Das Ergebnis der Betrachtung der Einzelrisiken ist eine *Risikomatrix*[57], siehe Abbildung 3.

[47] Vgl. Romeike, 2018, S. 10, 38; Schmola, 2016, S. 306.
[48] Vgl. Romeike, 2018, S. 40; Glage/Grötzner, 2016, Rn. 57; Schmola, 2016, S. 307; Dillerup, 2013, S. 886.
[49] Vgl. Brauweiler, 2019, S. 8; Dillereup, 2013, S. 886.
[50] Vgl. Romeike, 2018, S. 36; Schmola, 2016, S. 307.
[51] Vgl. Romeike, 2018, S. 36.
[52] Vgl. Brauweiler, 2019, S. 8; Glage/Grötzner, 2016, Rn. 61; Schmola, 2016, S. 307f.
[53] Vgl. Dillerup, 2013, S. 887.
[54] Vgl. Schomola, 2016, S. 307f.
[55] Vgl. Dillerup, 2013, S. 887.
[56] Vgl. Schmola, 2016, S. 308.
[57] Vgl. Brauweiler, 2019, S. 9f; Romeike, 2018, S. 41; Schmola, 2016, S. 308.

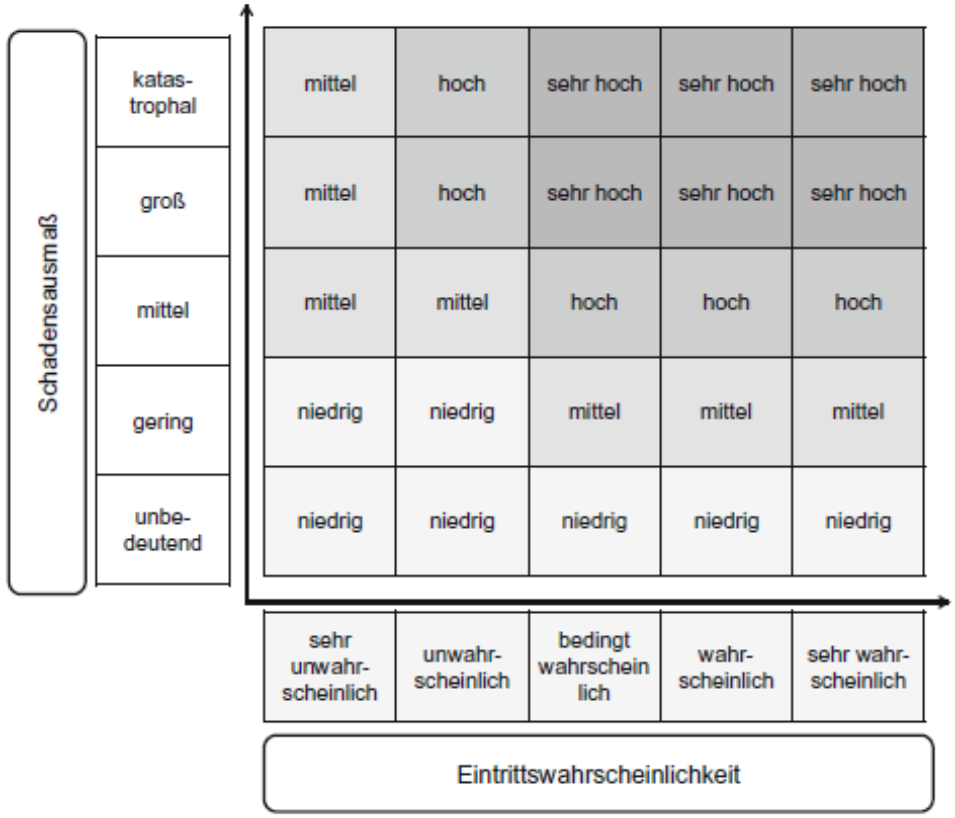


Abbildung 3: Risikomatrix[58]

Die Risikomatrix soll als Instrument bei der Prioritätensetzung helfen, wobei sie verschiedene Toleranzbereiche aufweist: Sie differenziert in kleine, also vertretbare Risiken, bedingt vertretbare (mittlere) Risiken und nicht vertretbare (große) Risiken.[59] Durch die grafische Darstellung und eine mögliche Farbgestaltung gelingt der Risikomatrix ein Gesamtüberblick über das Risikoportfolio sowie der Abbau der Komplexität verschiedener Risiken.[60]

Die *Risikobewältigung* initiiert geeignete Steuerungsmaßnahmen zur Beeinflussung der analysierten Risiken.[61] Möglich sind die Vermeidung von Risiken, die Verminderung der Auswirkungen von Risiken, der Transfer von Risiken und die Risikovorsorge.[62] Auch ein bewusstes Eingehen von Risiken ist an dieser Stelle möglich. Im Anschluss wird die Eignung der BSC als Instrument des Risikomanagements erläutert.

[58] Vgl. Schmola, 2016, S. 308.
[59] Vgl. Pauthner/Stephan, 2016, Rn. 118ff; Schmola, 2016, S. 309.
[60] Vgl. Romeike, 2018, S. 41; Schmola, 2016; S. 309.
[61] Vgl. Glage/Grötzner, 2016, Rn. 65f; Pauthner/Stephan, 2016, Rn. 38; Schmola, 2016, S. 309.
[62] Vgl. Schmola, 2018, S. 309; Dillerup, 2013, S. 888.

IV. Übertragung der BSC in das Risikomanagement

Im Folgenden werden Funktion und Aufbau der klassischen Balanced Score Card sowie deren mögliche Übertragung in das Risikomanagement erläutert.

1. Klassische BSC

Die *Balanced Score Card* wurde ursprünglich als Messinstrument für den Unternehmenserfolg entwickelt und hat sich mittlerweile in verschiedenen Bereichen als Hilfsmittel zur Definition und Überwachung von Zielen etabliert.[63] Während traditionelle Leistungsmesssysteme rein finanzwirtschaftlich ausgerichtet sind, werden bei der BSC auch nichtmonetäre Größen einbezogen, um eine ganzheitliche Sichtweise auf ein Unternehmen zu ermöglichen und somit als Informationssystem zu fungieren.[64] Dabei ist zu erwähnen, dass die BSC mehr als nur eine ad-hoc-Sammlung von finanziellen und nichtfinanziellen Leistungsmessern ist. Sie kann die Mission und Strategie einer Geschäftseinheit in materielle Ziele und Kennzahlen übersetzen, da sie aus einem top-down-Prozess hergeleitet wird.[65] So wurde die BSC zu einem strategischen Managementsystem weiterentwickelt, welches mithilfe ausgewogener mehrdimensionaler Kennzahlen zur Unternehmensbeurteilung und -steuerung versucht die Lücke zwischen Formulierung der Strategie und den operativen Maßnahmen zu schließen.[66] Sie ist also eine spezielle Art der Konkretisierung, Darstellung und Verfolgung von Strategien und übersetzt Mission und Strategie in Ziele und Kennzahlen, während sie – wie in Abbildung 4 dargestellt – in vier *Perspektiven* unterteilt ist.[67]

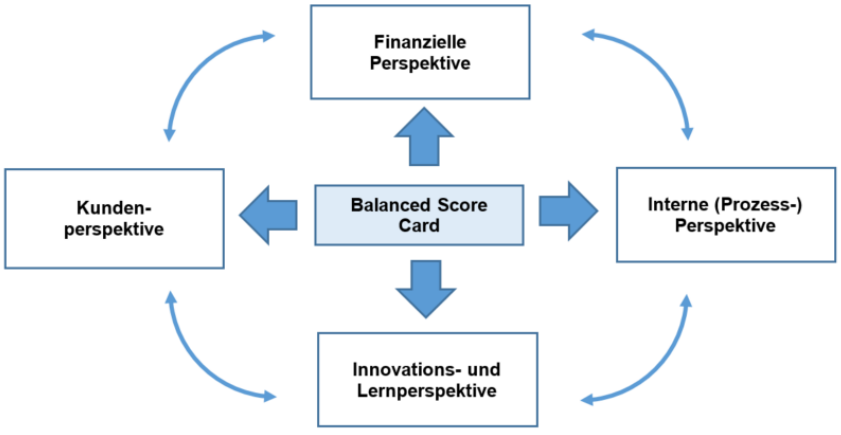


Abbildung 4: Klassische Perspektiven der BSC (eigene Darstellung)[68]

[63] Vgl. Kneisel, 2017, S. 256.
[64] Vgl. Kaplan/Norton, 2018, S. 8f, 20f; Heimer, 2007, S. 18f.; Henseler/Johen/Lingau, 2006, S. 14.
[65] Vgl. Kaplan/Norton, 2018, S. 9.
[66] Vgl. Kaplan/Norton, 2018, S. 8ff, Gleißner/Romeike, 2015, S. 548; Heimer, 2007, S. 18f; Gilles, 2002, S. 21f.
[67] Vgl. Kaplan/Norton, 2018, S. 23.
[68] Vgl. Kaplan/Norton, 2018, S. 9ff, S. 42.

Der klassische Ansatz der BSC umfasst somit die Betrachtung aus den folgenden vier Perspektiven: der finanziellen Perspektive, der Kundenperspektive, der internen (Prozess-)Perspektive sowie der Innovations- und Lernperspektive. Auf Basis der Betrachtung aus diesen vier Perspektiven soll die Unternehmensstrategie mithilfe einer klaren Struktur in konkrete Ziele übersetzt werden, was der Reduktion, Selektion und Konzentration einer Vielzahl möglicher strategischer Ziele dient.[69] Dabei wird eine Balance zwischen extern orientierten Messgrößen für Teilhaber und Kunden sowie internen Maßnahmen für Geschäftsprozesse, Innovationen sowie Lernen und Wachstum sichergestellt.[70]

Mit der Anwendung der BSC werden Ziele, Messgrößen und strategische Aktionen anhand entsprechender *Leitfragen* jeweils einer konkreten Betrachtungsweise zugeordnet.[71] In Abbildung 5 werden die jeweiligen Leitfragen und Inhalte der einzelnen Perspektiven dargestellt.

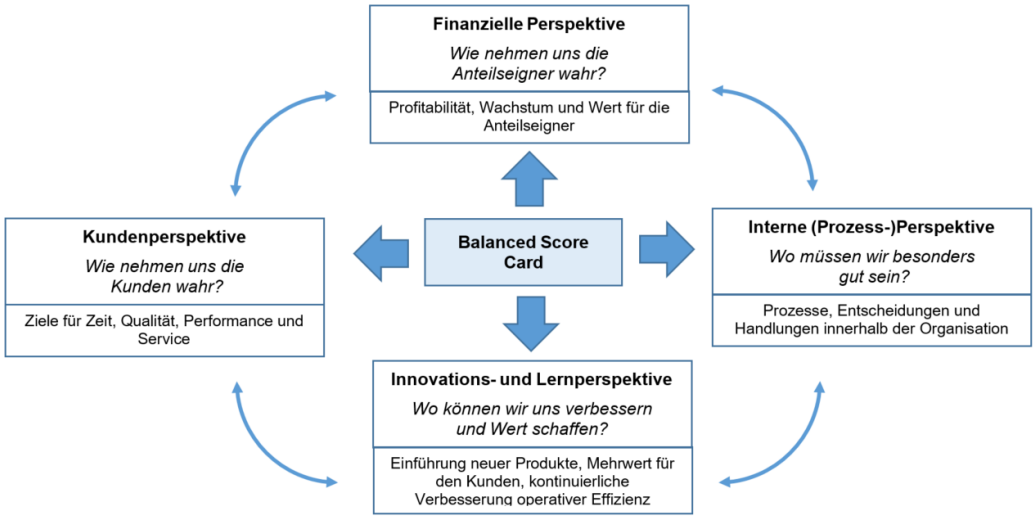


Abbildung 5: Klassische Perspektiven der BSC, Leitfragen und Inhalte (eigene Darstellung)[72]

So befasst sich die finanzielle Perspektive mit der Wahrnehmung der Anteilseigner. Profitabilität, Wachstum und Wert für die Anteilseigner sind die Inhalte dieser Perspektive. Mit der Wahrnehmung der Kunden beschäftigt sich die Kundenperspektive. Inhaltlich relevant sind hier Ziele für Zeit, Qualität, Performance und Service. Die interne (Prozess-)Perspektive befasst sich mit der Fragestellung in welchem Bereich man besonders gut sein muss.

[69] Vgl. Horváth & Partners, 2007, S. 44f, S. 156.
[70] Vgl. Kaplan/Norton, 2018, S. 9f.
[71] Vgl. Horváth & Partners, 2007, S. 2f; Zimmermann/Jöhnk, 2002, S. 57.
[72] Vgl. Kaplan/Norton, 2018, S. 9ff, S. 42.

Relevant sind an dieser Stelle Prozesse, Entscheidungen und Handlungen innerhalb der Organisation. Mit Verbesserung und Wertschaffung befasst sich die Innovations- und Lernperspektive, indem sie sich mit Einführung neuer Produkte, Mehrwert für den Kunden und kontinuierliche Verbesserung operativer Effizienz beschäftigt.[73]

Wichtig ist die *Verknüpfung* der einzelnen Perspektiven durch eine Kette von Ursache-Wirkungsbeziehungen.[74] Sie sollten nicht isoliert, sondern als voneinander abhängend, gleichgewichtig und ausgewogen betrachtet werden[75], um das Unternehmen in der Gesamtschau darstellen zu können. Dargestellt wird die gegenseitige Wechselbetrachtung bei gleichzeitiger Betrachtung im Gesamten in den Abbildungen 4 und 5 durch Pfeile. Fähigkeiten und Wissen der Mitarbeiter, welche der Innovations- und Lernperspektive zugeordnet werden, wirken sich auf die Prozessabläufe, -qualität und -zeit aus, welche der internen (Prozess-)Perspektive angehören. Diese bestimmen wiederum die Qualität der Unternehmensleistung für den Kunden und seine Zufriedenheit, ersichtlich in der Kundenperspektive. Die Kundentreue hat Einfluss auf das finanzielle Ergebnis, welches in der Finanzperspektive dargestellt wird. Die finanzielle Perspektive ist dabei der Endpunkt der Ursache-Wirkungsbeziehung.[76] Diese Fokussierung basiert auf der Annahme, dass der langfristige finanzielle Erfolg das oberste Unternehmensziel ist.

Der *Prozess der Zielableitung* bei der klassischen BSC wird in Abbildung 6 dargestellt.

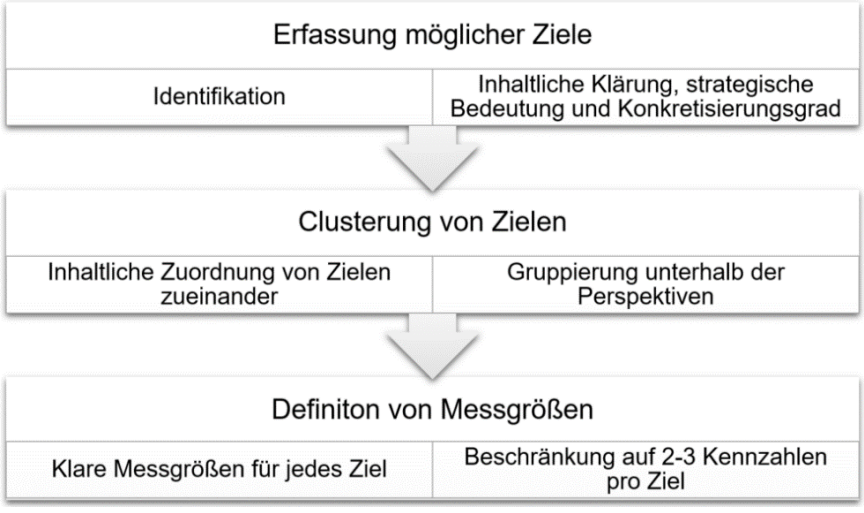


Abbildung 6: Prozess der Zielableitung bei der klassischen BSC, eigene Darstellung[77]

[73] Vgl. Kaplan/Norton, 2018, S. 9ff, S. 42.
[74] Vgl. Kaplan/Norton, 2018, S. 28f, 143; Heimer, 2007, S. 21f.
[75] Vgl. Krisper, 2009, S. 9; Horváth & Partners, 2007, S. 41.
[76] Vgl. Zimmermann/Jöhnk, 2002, S. 57f.
[77] Vgl. Kneisel, 2017, S. 257.

Die Ziele der jeweiligen Perspektive werden zunächst identifiziert, inhaltlich ausgearbeitet und geclustert, um anschließend gegenwarts- und zukunftsorientierten Kennzahlen für jedes strategische Ziel zu definieren.[78] Nach der Zielableitung sind Maßnahmen festzulegen, durch welche die Vorgabewerte und damit die strategischen Ziele erreicht werden sollen.[79]
Die Perspektiven der BSC können um strategische Ziele, Messgrößen, Zielwerte und strategische Aktionen ergänzt werden, siehe Tabelle 1.

Tabelle 1: Inhalte zur Definition der Messgrößen der BSC (eigene Darstellung)[80]

Perspektive			
Leitfrage			
Inhalte			
Strategisches Ziel	Messgröße	Zielwert	Strategische Aktion

Die *Kennzahlen* halten die Balance zwischen den Messgrößen der Ergebnisse vergangener Tätigkeiten und den Kennzahlen, welche zukünftige Leistungen antreiben sollen. Dabei ist sie ausgewogen in Bezug auf objektive, leicht zu quantifizierende Ergebniskennzahlen und subjektive, urteilsabhängige Leistungstreiber und Ergebniskennzahlen.[81] Mögliche Kennzahlen der Finanzperspektive sind return on investment und economic value-added. Die Kundenperspektive kann anhand Zufriedenheit, Treue, Markt- und Kundenanteil gemessen werden. Relevant für die interne (Prozess-)Perspektive sind Qualität, Reaktionszeit, Kosten und Einführung neuer Produkte. Für die Innovations- und Lernperspektive werden Mitarbeiterzufriedenheit und Zugriff auf Informationssysteme betrachtet.

Die BSC bietet dem Management also ein umfassendes Instrumentarium, um die Unternehmensvision und -strategie in ein geschlossenes Bündel von Leistungsmessfaktoren zu übertragen.[82] Die strategischen Zielsetzungen und Zusammenhänge werden konzentriert und für alle Beteiligten leicht verständlich dargestellt. Einseitiges Denken bei der Aufstellung und Verfolgung der

[78] Vgl. Kaplan/Norton, 2018, S. 13ff; Kneisel, 2017, S. 257; Zimmermann/Jöhnk, 2002, S. 57.
[79] Vgl. Zimmermann/Jöhnk, 2002, S. 57.
[80] Vgl. Kaplan/Norton, 2018, S. 23.
[81] Vgl. Kaplan/Norton, 2018, S. 9.
[82] Vgl. Kaplan/Norton, 2018, S. 23.

Ziele wird durch die Zuordnung zu unterschiedlichen Perspektiven verhindert. Das Finden der geeigneten Kennzahlen zur Messung strategischer Ziele ist allerdings nicht einfach. Weiter bietet die klassische BSC, abgesehen von der Kundenperspektive, keinen Bezug zur Unternehmensumwelt und scheint daher nicht besonders ausgewogen zu sein. Während bei der Betrachtung der Ursache-Wirkungsbeziehungen die Interessen der Eigner im Vordergrund stehen, werden andere Stakeholder wie Mitarbeiter oder Lieferanten vernachlässigt, weshalb die Erweiterung um zusätzliche Perspektiven empfohlen wird.[83]

2. BSC im Risikomanagement

Risiken sollten nicht isoliert, sondern unmittelbar im Kontext aller unternehmerischen Entscheidungen betrachtet werden.[84] Für ein effizientes Risikomanagement ist es unerlässlich Instrumentarien, welche die Umsetzung eines integrativen Risikomanagements wirkungsvoll unterstützen, zu nutzen.[85] Die BSC bietet sich als ein solches Instrument an, da sie gleichzeitig als Planungs-, Steuerungs-, Kontroll- und Informationsinstrument fungieren kann.[86] Um die BSC auch für das Risikomanagement nutzbar zu machen, werden in der Literatur *verschiedene Modifikationen* vorgeschlagen.[87] Vereinfacht dargestellt sind diese Integration, Erweiterung und Weiterentwicklung der klassischen BSC. Die *Integration,* siehe Abbildung 7, ist die vollständige Einordnung und Subsumtion von Risikokennzahlen unter die vier klassischen Perspektiven der BSC des Unternehmens.[88]

[83] Vgl. Dillerup/Stoi, 2013, S. 398.
[84] Vgl. Gleißner/Romeike, 2015, S. 548.
[85] Vgl. Heimer, 2007, S. 29.
[86] Vgl. Gleißner/Romeike, 2015, S. 548; Heimer, 2007, S. 29.
[87] Vgl. Hunziker/Fallegger/Jovic, 2018; Gleißner/Romeike, 2015, S. 548ff; Krisper, 2009, S. 31ff; Heimer, 2007, S. 31ff; S. 54ff; Zimmermann/Jöhnk, 2002, S. 58.
[88] Vgl. Kneisel, 2017, S. 258; Weber/Weißenberger/Liekweg, 1999, S. 1710.

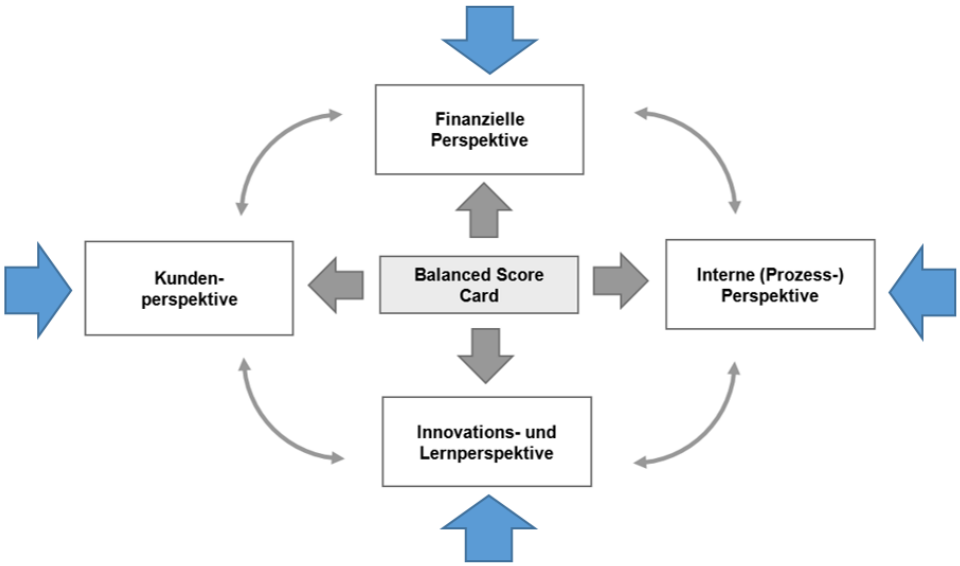


Abbildung 7: Integration der Risikokennzahlen in die klassische BSC (eigene Darstellung)[89]

Dabei werden Verantwortlichkeiten klar geregelt und die verschiedenen Risiken können durch die Verknüpfung der Perspektiven in einer zusammenhängenden Ursache-Wirkungskette abgebildet werden.[90] Allerdings können den originären Perspektiven nicht eindeutig zuordenbare Risiken bei diesem Ansatz nicht berücksichtigt werden.[91]

Bei der Modifikationsmöglichkeit der *Erweiterung* könnte die klassische BSC um eine zusätzliche Risikoperspektive ergänzt werden[92], siehe Abbildung 8.

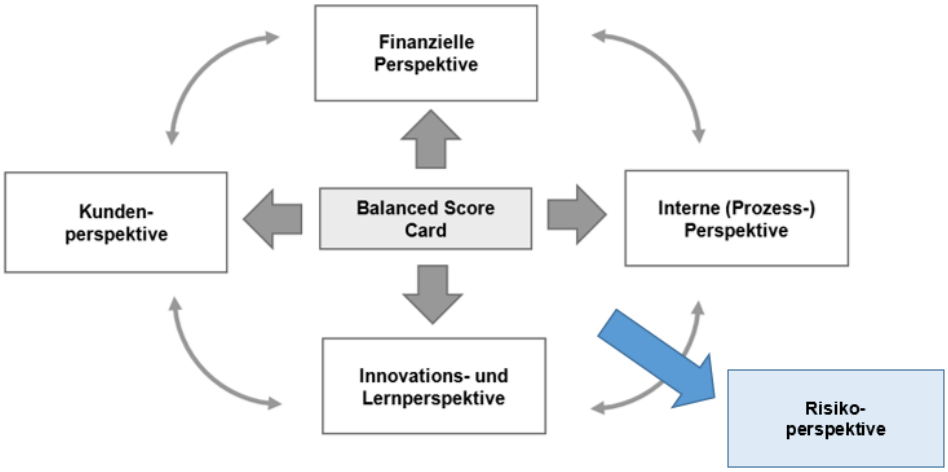


Abbildung 8: Erweiterung der klassischen BSC (eigene Darstellung)[93]

[89] Vgl. Kneisel, 2017, S. 258.
[90] Vgl. Gleißner/Romeike 2015, S. 551; Heimer, 2007, S. 33.
[91] Vgl. Gleißner/Romeike 2015, S. 551; Krisper, 2009, S. 40.
[92] Vgl. Teichmann/Erkens, 2000, S. 28ff; Wagner, 2000, S. 87ff.
[93] Vgl. Kneisel, 2017, S. 258.

Damit wird das Risikocontrolling – also die Identifizierung, Bewertung, Steuerung, Kommunikation und Kontrolle von Risiken – in die klassische BSC integriert. Problematisch könnte hier sein, dass die Ursachen-Wirkungsbeziehungskette durch die Betrachtung heterogener Risiken in nur einer einzigen zusätzlichen Risikoperspektive durchbrochen werden könnte.[94] Die Risiken werden den einzelnen Perspektiven nicht eindeutig zugeordnet, was ein Vorteil sein kann, da sich nicht alle Risiken einer der traditionellen Perspektiven zuordnen lassen. Ebenso können sie in einer zentralen Darstellung durch die separaten Risikoperspektive vollständig dargestellt werden.[95] Die Modifizierung mittels *Ableitung* wird im nächsten Abschnitt erläutert.

3. Risiko-BSC

Bei der *Ableitung* wird aus der übergeordneten BSC des Unternehmens eine spezielle Risiko-BSC abgleitet[96], siehe Abbildung 9.

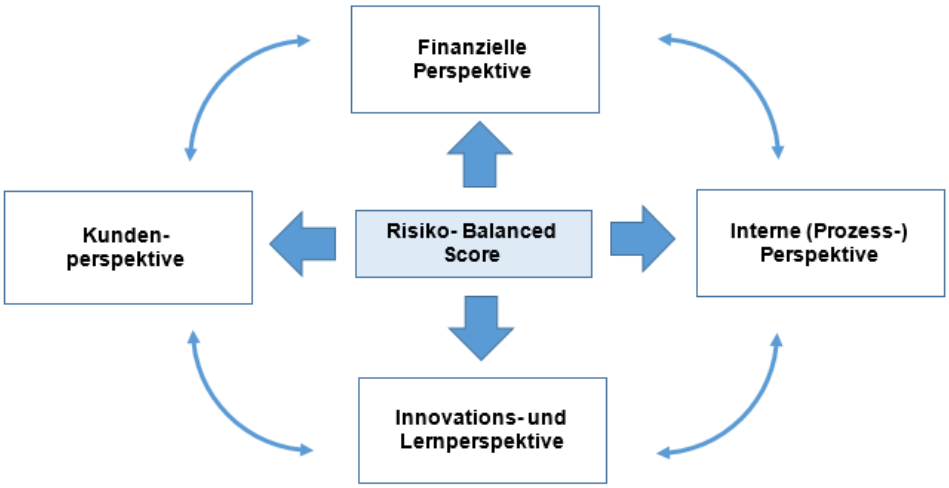


Abbildung 9: Ableitung einer Risiko-Balanced Score Card
(eigene Darstellung)[97]

Die Risiko-BSC ermöglicht die systematische Erfassung von Risiken sowie deren Eintrittswahrscheinlichkeiten und Schadenshöhe. Auf dieser Grundlage basierend können Maßnahmen zur Risikominderung festlegt werden. Da wie bereits beschrieben die BSC ein Hilfsmittel im Umgang mit der Unternehmensstrategie ist und das Risikomanagement ebenfalls eine strategische

[94] Vgl. Krisper, 2009, S. 45; Zimmermann/Jöhnk, 2002, S. 58.
[95] Vgl. Gleißner/Romeike 2015, S. 551; Hombug/Stephan/Haupt, 2005, S. 1074.
[96] Vgl. Kneisel, 2017, S. 258; Zimmermann/Jöhnk, 2002, S. 58.
[97] Vgl. Kneisel, 2017, S. 258.

Ausrichtung benötigt ist die Anwendung einer Risiko-BSC denkbar. Abschließend könnte man die Risiko-BSC mit der klassischen BSC des Unternehmens zum strategischen Management verbinden.

Die *Perspektiven* der klassischen BSC werden bei der Risiko-BSC beibehalten, da diese eine ganzheitliche Sichtweise auf das Unternehmen ermöglichen. Leitfragen und Inhalte müssen bei der Risiko-BSC jedoch angepasst werden, siehe Abbildung 10. Möglich ist dies, da die klassische BSC und deren Perspektiven kein starres Konzept abbilden, sondern individuell auf das Unternehmen zugeschnitten sind und somit unternehmensspezifisch angepasst und ergänzt werden können.[98]

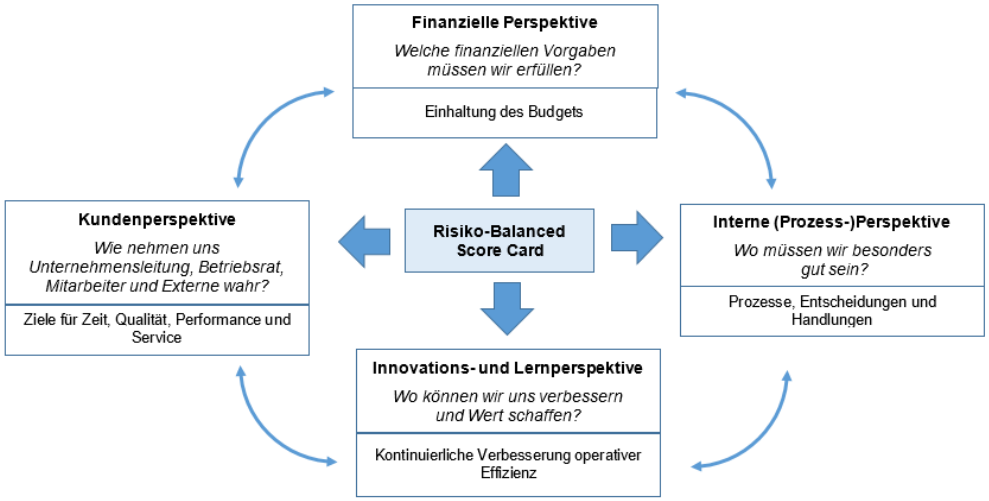


Abbildung 10: Perspektiven der Risiko-BSC, Leitfragen und Inhalte

Die *Leitfragen* der finanziellen Perspektive und der Kundenperspektive müssen hierzu angepasst werden. Die Leitfrage der finanziellen Perspektive verändert sich von „Wie nehmen uns die Anteilseigner wahr?“ zu „Welche finanziellen Vorgaben müssen wir erfüllen?“. Bei der Kundenperspektive werden die Stakeholder von Kunden zu Unternehmensleitung, Betriebsrat, Mitarbeitern und Externen verändert.

Die *Inhalte* der Risiko-BSC im Vergleich zur klassischen BSC müssen in der finanziellen Perspektive und der Innovations- und Lernperspektive angepasst werden. Die Finanzperspektive befasst sich nun mit der Einhaltung des vorgegebenen Budgets und nicht mehr mit Profitabilität, Wachstum und Wert für die Anteilseigner. Die Innovations- und Lernperspektive wird reduziert

[98] Vgl. Krisper, 2009, S. 10.

auf die kontinuierliche Verbesserung operativer Effizienz, sodass die Einführung neuer Produkte und der Mehrwert für die Kunden wegfallen.
Der *Prozess der Risikoableitung* ähnelt zu Beginn dem der Zielableitung der klassischen BSC, siehe Abbildung 11.

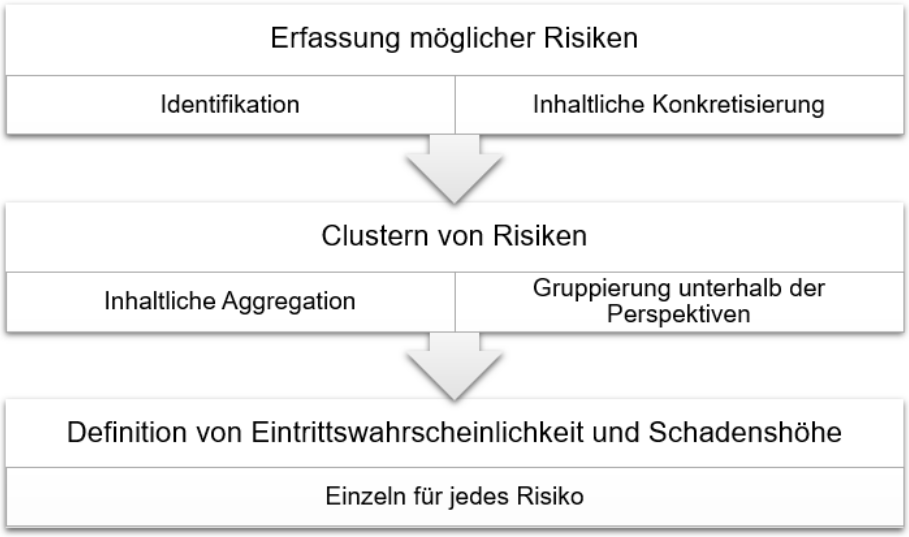


Abbildung 11: Prozess der Risikoableitung bei der Risiko-BSC

Zunächst werden die Risiken unter Zuhilfenahme der vier Perspektiven der klassischen BSC systematisch erfasst, indem diese zunächst identifiziert, aggregiert und den vier Perspektiven zugeordnet werden. Der Prozess der Risikoableitung bei der Risiko-BSC ähnelt dem operativen Risikomanagementprozess, siehe Kapitel A. III. Somit scheint es an dieser Stelle sinnvoll die Risiko-BSC als Instrument zur Risikoidentifizierung, -analyse, -bewertung zu nutzen. Die Messgrößen sollten aber verändert werden, siehe Tabelle 2.

Tabelle 2: Inhalte zur Definition der Messgrößen der Risiko-BSC (eigene Darstellung)

Perspektive		
Leitfrage		
Inhalte		
Risikoursache	Eintritts-wahrscheinlich-keit	Schadens-höhe

Anstelle der Definition von Messgrößen folgt in diesem Fall eine Analyse der Eintrittswahrscheinlichkeit und Schadenshöhe der Risiken. Dieser An-

satz wird gewählt, da hier der Umgang mit Risiken und nicht mit strategischen Zielen erprobt wird. Detaillierte Ausführungen zur Messung von Risiken lassen sich in Kapitel A. III. Risikomanagement finden.

V. Zwischenergebnis

Im Rahmen der Überwachung ihrer Compliance-Risiken sollten Unternehmen den relevanten Rechtsrahmen sowie mögliche Änderungen identifizieren und bewerten. Da sich Parallelen zwischen CMS und Risikomanagement erkennen lassen, scheint es sinnvoll Methoden des Risikomanagements bei der Identifizierung und Bewertung von Risiken aus dem Compliance-Bereich zu nutzen. Eine Risiko-BSC ist eine strategische Methode im Umgang mit Risiken, welche dem Unternehmen eine ganzheitliche Sichtweise bietet. Die Einführung des neuen HinSchG könnte Risiken für Unternehmen bergen. Nachfolgend wird geprüft, ob die Risiko-BSC in diesem Zusammenhang ein geeignetes Mittel im Umgang mit Risiken, welche sich aus der Umsetzung des HinSchG ergeben, sein kann.

B. Rechtliche Unsicherheiten aus dem HinSchG

Nun werden ausgewählte rechtliche Unsicherheiten herausgearbeitet, mit welchen Unternehmen bei der Umsetzung des HinSchG konfrontiert werden könnten. In der folgenden Betrachtung der Themenfelder persönlicher und sachlicher Anwendungsbereich, Anreize zur Wahl der internen Meldestelle, zentrale Konzernmeldestelle, anonyme Meldungen, Schutzvoraussetzungen, Repressalienverbot und Beweislastumkehr, Ausnahmen vom Vertraulichkeitsgebot sowie interne Untersuchungen als Folgemaßnahme wird sich auf interne Meldestellen in privatrechtlichen Unternehmen beschränkt.

I. Persönlicher Anwendungsbereich

§ 1 HinSchG definiert hinweisgebende Personen als natürlichen Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese an die nach diesem Gesetz vorgesehenen Meldestellen melden oder offenlegen. Nicht geschützt werden Personen, die in einem privaten Rahmen Kenntnis über Rechtsverstöße erlangen und diese melden. Unternehmen könnten jedoch durchaus ein Interesse an solchen Meldungen haben, sodass diese Personen auch durch das HinSchG geschützt werden sollten.[99] Ohne Schutz könnten relevante Informationen über mögliche Verstöße für Unternehmen verloren gehen.

Neben hinweisgebenden Personen werden vom HinSchG gem. § 1 Abs. 2 Personen geschützt, die *Gegenstand einer Meldung oder Offenlegung* sind sowie sonstige von einer Meldung oder Offenlegung *betroffene Personen*. Beide Personengruppen finden in den Schutzmaßnahmen der §§ 33 ff. HinSchG außer in § 38 keine Erwähnung. § 38 HinSchG sieht vor, dass die hinweisgebende Person nach vorsätzlicher oder grob fahrlässiger Abgabe einer unrichtigen Meldung zum Schadensersatz gegenüber Personen, die Gegenstand der Meldung sind oder von ihr betroffen sind, verpflichtet ist. Die meisten hinweisgebenden Personen geben falsche Hinweise gutgläubig und gerade nicht vorsätzlich oder grob fahrlässig ab; dadurch liegt nahe, dass eine von einem solchen Hinweis betroffene Person einen auf § 38 HinSchG gestützten Schadensersatzprozess sehr wahrscheinlich verlieren könnte.[100] Bei

[99] Vgl. Dilling, 2022, S. 145; Lüneborg, 2022/1, S. 379; Nießen, 2022, S. 400; a.A. Bundesverband für Unternehmensjuristen, 2022, S. 3.
[100] Vgl. Dilling, 2022, S. 151.

der Aufarbeitung der Hinweise können betroffene Personen erhebliche (irreparable) finanzielle und psychologische Schäden sowie Reputationsschäden erleiden[101], gerade weil es an verlässlichen Verfahrensregeln für interne Ermittlungen fehlt[102]. Die Regelung von Verfahrensrechten für die o.g. Personengruppen dürfte auch für Unternehmen sinnvoll sein.[103] Wenn Mitarbeiter als betroffene Person schlechte Erfahrungen machen und diese mit den Kollegen teilen, könnte sich dies in mangelndem Vertrauen in das das Hinweisgebersystem und das Compliance Management System widerspiegeln. Eine wahrgenommene Ineffektivität der Maßnahmen könnte sich auf die Unternehmenskultur und die Reputation auswirken.

Obwohl die beruflichen Perspektiven der hinweisgebenden Person durch das HinSchG bewahrt und dessen berufliches Umfeld geschützt werden sollen[104], sind *verbundene natürliche Personen* vom persönlichen Anwendungsbereich in § 1 HinSchG nicht erfasst. Gem. § 34 Abs. 1 HinSchG gelten aber die Schutzmaßnahmen der §§ 35 bis 37 für natürliche Personen, die die hinweisgebende Person bei einer Meldung oder Offenlegung im beruflichen Zusammenhang vertraulich unterstützen. Gem. § 34 Abs. 2 Nr. 1 HinSchG gelten die §§ 35 bis 37 ebenfalls für Dritte, die mit der hinweisgebenden Person in Verbindung stehen und in einem beruflichen Zusammenhang Repressalien erlitten haben, es sei denn, diese beruhen nicht auf der Meldung oder Offenlegung durch die hinweisgebende Person. Basierend auf Art. 4 Abs. 4 WBRL liegt das Telos des § 34 HinSchG darin, mögliche Hürden für die Abgabe von Hinweisen zu vermeiden. Hinweisgebende Personen könnten aus Angst vor Nachteilen für nahestehende Dritte aber von einer Meldung abgehalten werden. Auch könnten potenzielle Unterstützer aus Angst vor Repressalien abgeschreckt werden und somit das Whistleblowing mangels Unterstützung unterbleiben.[105]

Schwierig gestaltet sich die die *Abgrenzung der verbundenen natürlichen Personen* und somit die Frage, ob für diese der persönliche Schutzbereich des HinSchG der eröffnet ist. Die in § 34 Abs. 1 HinSchG genannten Personen könnten in Anlehnung an Art. 4 Abs. 4 lit. a i.V.m. Art. 5 Nr. 8 und ErwG 41 S. 2 WBRL Gewerkschafts- und Arbeitnehmervertreter sein, die

[101] Vgl. Thüsing/Forst, 2021, § 6 Rz. 65.
[102] Vgl. Hauschka/Moosmayer/Lösler, 2016, § 46 Rz. 4.
[103] Vgl. Dilling, 2022, S. 151.
[104] Vgl. Dilling, 2019, S. 216.
[105] Vgl. Fest in Franzen/Gallner/Oetker, 2022, RL (EU) 2019/1937, Art. 4, Rn. 25; 19, Rn. 1; Siemes, 2022, S. 10, 12; 2021 S. 71.

die hinweisgebende Person beraten oder ihr anderweitig behilflich sind.[106] Personen, die einer hinweisgebenden Person im beruflichen Kontext Informationen über Verstöße zukommen lassen, fallen nicht unter diese Kategorie[107] ebenso wie eine bloße seelische Bekräftigung durch Familienmitglieder im Privatbereich[108]. Für die beiden zuletzt genannten Personengruppen könnte in Anlehnung an Art. 4 Abs. 4 lit. b WBRL dessen Wirkung für Verwandte und Kollegen dem Wortlaut nach einschlägig sein.[109] Hervorzuheben ist an dieser Stelle, dass nur geschützt werden soll, wer mit der hinweisgebenden Person in Verbindung steht und in einem beruflichen Kontext Repressalien erleiden könnte. Wenn Dritte also im privaten Kontext von Gefahren und Verstößen erfahren, werden sie nicht geschützt. Diese werden regelmäßig nicht berufliche Repressionen fürchten müssen, sondern in anderen Formen wie z. B. durch Schadenersatzklagen oder Verunglimpfung benachteiligt werden.[110] Jedoch sind auch diese Meldungen für Unternehmen interessant und tragen zur Effektivität des Hinweisgebersystems bei.

II. Sachlicher Anwendungsbereich

Art. 2 der WBRL erlaubt den Mitgliedsstaaten den *sachlichen Anwendungsbereich* bei der Umsetzung auf nationales Recht auszuweiten. Neben Verstößen gegen von der WBRL erfasstes Unionsrecht umfasst das HinSchG gem. § 2 Abs. 1 auch Verstöße gegen korrespondierende nationale Vorschriften sowie nationale Strafvorschriften und bußgeldbewährte Vorschriften, soweit die Vorschrift dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient. Den Erwartungen an einen umfassenden Schutz von hinweisgebenden Personen wird das HinSchG mit seinem weiten sachlichen Anwendungsbereich gerecht.[111]

Dem entgegen steht, dass die Auswahl der Rechtsgebiete willkürlich erscheinen könnte. Kaum eine *hinweisgebende Person* dürfte ohne Rechtsrat in der Lage sein nachzuvollziehen, welche Verstöße jeweils in den sachlichen Anwendungsbereich fallen und so die vertrauliche Behandlung ihrer Identität

[106] Vgl. Siemes, 2022, S. 8; 2021, S. 70; Bundesrechtsanwaltskammer, 2022, S. 8; Gerdemann, 2021, S. 38; Colneric/Gerdemann, 2020, S. 34; a. A. Fest in Franzen/Gallner/Oetker, 2022, RL (EU) 2019/1937, Art. 4, Rn. 25, 28.
[107] Vgl. Siemes, 2022, S. 8; Transparency International, 2020, S. 27; a. A. Forst, 2020, S. 288 und Schmolke, 2020, S. 5f.
[108] Vgl. Siemes, 2022, S. 8; Bundesministerium der Justiz, 2020, S. 69.
[109] Vgl. Siemes, 2022, S. 8.
[110] Vgl. Dilling, 2019, S. 216f.
[111] Vgl. Bundesverband der Compliance Manager, 2022, S. 6; Gerdemann, 2022/2; S. 2; Steinhauser/Saalwächter-Hirsch, Trouvain, 2022, S. 330.

nach sich ziehen würden.[112] Der Entwurfsverfasser schlägt als Lösung für dieses Problem eine Anpassung der Rechtsbereiche vor. Diese sollen so angepasst werden, dass hinweisgebende Personen – unabhängig davon ob sich der Verstoß aus Landes- Bundes- oder Unionsrecht ergibt – einschätzen können, ob ein beobachtetes Verhalten gegen Vorschriften aus dem jeweiligen Bereich verstößt.[113] Eine Erläuterung wie die Rechtsgebiete angepasst werden sollen oder wie damit der hinweisgebenden Person geholfen sein soll gibt es an dieser Stelle nicht.[114] Viele potenzielle hinweisgebende Personen könnte die daraus resultierende Unsicherheit abschrecken, was zu einer Zurückhaltung der Meldung und damit zu einer Ineffektivität des Whistleblowersystems führen könnte. Hinweisgebende Personen können sich nicht ohne Weiteres sicher sein, dass sie und ihre Identität vom HinSchG geschützt werden. Nach § 8 Abs. 1 Nr. 1 HinSchG ist die Vertraulichkeit der Identität der gutgläubigen hinweisgebenden Person geschützt, weitere Ausführungen hierzu lassen sich in Kapitel VI. Schutzvoraussetzungen finden.

Auch für die Mitarbeiter der *internen Meldestelle* dürfte es trotz möglicher juristischer Vorbildung bei der Vielzahl der Rechtsgebiete schwierig sein, hinweisgebenden Personen in jedem Fall eine verlässliche Rückmeldung zum sachlichen Anwendungsbereich zu geben.[115] Gem. § 17 Abs. 1 Nr. 2 HinSchG prüft die interne Meldestelle, ob der gemeldete Verstoß in den sachlichen Anwendungsbereich nach § 2 fällt. Wenn die interne Meldestelle den Anwendungsbereich falsch beurteilt und zu Unrecht einen Schutz bejaht oder versagt, könnte das zu Haftungsrisiken führen.[116] Ein IT-gestütztes Hinweisgebersystem dürfte angesichts der Komplexität des sachlichen Anwendungsbereichs (noch) nicht in der Lage dazu sein in jedem Fall rechtssicher und anwendungsfreundlich zu bestimmen, ob eine Meldung in den sachlichen Anwendungsbereich des HinSchG fällt oder nicht.[117] Zur Unterstützung der für die Entgegennahme und Beurteilung der Meldung zuständigen Personen könnte man den hinweisgebenden Personen eine technische Vorauswahlmöglichkeit der vom sachlichen Anwendungsbereich des HinSchG erfassten Rechtsgebiete anbieten. Fraglich ist aber, ob das eine ausreichende

[112] Vgl. BT-Drs. 20/5992, S. 42; Bundesregierung, 2023, FH zum HinSchG, S. 48; Bundesregierung, 2022, RegE zum HinSchG, S. 65; Deutscher Anwaltsverein, 2022, S. 8; Dilling, 2022, S. 145f; Nießen, 2022, S. 400; Transparency International, 2022; S. 3.
[113] Vgl. BT-Drs. 20/5992, S. 42; Bundesregierung, 2023, FH zum HinSchG, S. 48; Bundesregierung, 2022, RegE zum HinSchG, S. 65.
[114] Vgl. Dilling, 2022, S. 146.
[115] Vgl. Dilling, 2022, S. 146; Transparency International, 2022; S. 3.
[116] Vgl. Dilling, 2022, S. 146.
[117] Vgl. Dilling, 2022, S. 146.

Hilfestellung wäre. Außerdem werden Meldungen auch über andere Kanäle wie Telefongespräche, E-Mails, Briefe oder persönliche Gespräche eingehen. Technische Hilfsmittel oder zusätzliche Schulungen für das Personal der internen Meldestellen dürften mit finanziellem und organisatorischem Mehraufwand einhergehen.

Bereits die *Legalitätspflicht* verpflichtet Unternehmen zu rechtskonformem Verhalten.[118] Damit ist jeder begründete Hinweis auf einen Verstoß gegen nationales Recht von Unternehmen zu verfolgen. Die interne Meldestelle wird somit verpflichtet sein auch solche Hinweise an die Unternehmensleitung weiterzugeben, die nicht in den sachlichen Anwendungsbereich des HinSchG fallen. An dieser Stelle wäre es sachgerecht, den Schutz hinweisgebender Personen so weit reichen zu lassen wie die Legalitätspflicht des Unternehmens, damit das Hinweisgebersystem effektiv sein kann.[119] Diese Effektivität ist eine geeignete Aufsichtsmaßnahme i.S.v. § 130 Abs. 1 OWiG[120], weswegen Unternehmen bei einem Verstoß mit Bußgeldzahlungen rechnen müssen.[121]

Weiter wird kritisiert, dass *Verstöße gegen unternehmensinterne (Compliance-)Vorgaben* nicht in den sachlichen Anwendungsbereich des HinSchG fallen, obwohl auch sie Gegenstand von Meldungen sein können.[122] Auch Verstöße gegen unternehmensinterne Regelungen können erhebliche Konsequenzen für die Unternehmensleitung haben; Beispiele hierfür sind deliktische Haftungsansprüche oder die Verletzung von Sorgfaltspflichten.[123] Es ist davon auszugehen, dass interne Meldestellen Verstöße gegen unternehmensinterne Regelungen wegen der Legalitätspflicht des Unternehmens weiterleiten werden. Auch sind hinweisgebende Personen, die Verstöße gegen unternehmensinternes Recht melden der Gefahr von Repressalien ausgesetzt und somit nicht weniger schützenswert.[124] Dadurch könnten potenzielle hinweis-

[118] Vgl. Dilling, 2022, S. 146; Freidank, 2022, S. 1872; Dilling, 2021, S. 63; Taschke, 2021, S. 86; Colneric/Gerdemann, 2020, S. 137; Schmolke, 2020, S. 11.
[119] Vgl. Deutscher Anwaltsverein, 2022, S. 8; Dilling, 2022, S. 146; Freidank, 2022, S. 1872; Lüneborg, 2022/1, S. 379.
[120] Vgl. Dilling, 2022, S. 149; Freidank, 2022, S. 1872f.
[121] Vgl. BGH, Urt. v. 09.05.2017 – 1 StR 265/16 (Panzerhaubitze) = BeckRS 2017, 114578, Rz. 118.
[122] Vgl. Colneric/Gerdemann, 2022, S. 162; Dilling, 2022, S. 146.
[123] Vgl. Supreme Court of the United Kingdom 12.02.2021 - Okpabi and others v Royal Dutch Shell Plc and another, https://www.supremecourt.uk/cases/uksc-2018-0068.html (zuletzt aufgerufen am 18.03.2023); OLG Hamm 29.5.2019 – AZ 8 U 146/18, BeckRS 14258, Rz. 60.
[124] Vgl. Dilling, 2022, S. 146.

gebende Personen aus Angst vor unzureichendem Schutz abgeschreckt werden, wodurch mögliche relevante Hinweise ausbleiben und somit einem wirksamen Whistleblowersystem im Weg stehen.

III. Anreize zur Wahl der internen Meldestelle

Grundsätzlich können gem. § 7 Abs. 1 S. 1 HinSchG Personen, die beabsichtigen, Informationen über einen Verstoß zu melden, wählen, ob sie sich an eine interne oder externe Meldestelle wenden. Nach § 7 Abs. 3 S. 1 HinSchG sollen Beschäftigungsgeber, die nach § 12 zur Einrichtung einer internen Meldestelle verpflichtet sind, Anreize dafür schaffen, dass sich hinweisgebende Personen vor einer Meldung an eine externe Meldestelle zunächst an die jeweilige interne Meldestelle wenden. Es sollen gem. § 7 Abs. 3 S. 2 HinSchG klare und leicht zugängliche Informationen über die Nutzung des internen Meldeverfahrens bereitgestellt werden, die Möglichkeit einer externen Meldung darf hierdurch gem. § 7 Abs. 3 S. 3 HinSchG aber nicht beschränkt oder erschwert werden. Erwähnenswert ist an dieser Stelle, dass Inhalte des Abs. 3 erst mit der Beschlussempfehlung des Rechtsausschusses Einzug in das HinSchG gefunden haben.[125] Die die attraktive Gestaltung interner Meldekanäle ist bereits jetzt gängige Unternehmenspraxis ist, um im Wettbewerb gegenüber den externen (behördlichen) Meldekanälen zu gewinnen.[126]

Mitarbeiter könnten durch Anreizsetzung und Vereinfachung der Nutzung interner Meldestellen motiviert werden, Missstände vorranging intern zu melden, bevor sie sich bei Behörden melden[127], wodurch Unternehmen durch frühe, schnelle und effektive interne Aufarbeitung und einer Strategie zum Umgang mit dem Fehlverhalten Geldbußen und Imageschäden vermeiden könnten.[128]

Die *Ausgestaltung* der Förderung ohne eine Verpflichtung zur Nutzung der internen Meldestelle bleibt durch den Gesetzgeber weitgehend offen. Möglichkeiten wären die Optimierung der internen Meldewege durch einfache Zugänglichkeit und Nutzerfreundlichkeit, eine gute Kommunikationskultur, die Förderung sozialer Verantwortung sowie das wirksame Vorgehen gegen

[125] Vgl. BT-Drs. 20/5992, S. 11; BT-Drs. 20/4909, S. 19.
[126] Vgl. Steinhauser/Saalwächter-Hirsch/Trouvain, 2022, S. 332.
[127] Vgl. Bundesverband der Deutschen Industrie, 2022, S.5f; Dzida/Granetzny, 2020, S. 1205.
[128] Vgl. Deutscher Anwaltsverein, 2022, S. 15; Thüsig/Musiol, 2022, S. 2420; Dzida/Granetzny, 2020, S. 1206.

Verstöße und den Schutz vor Repressalien.[129] Denkbar wären hier ebenfalls hohe IT-Sicherheitsvorkehrungen, die Schaffung höherer gesetzlicher Vertraulichkeitsstandards, etwa durch die Einschränkung von DSGVO-Auskunftsrechten der von der Meldung Betroffenen oder die Ausweitung der Kronzeugenregelung des § 26 b StGB.[130] Auch unternehmensinterne *finanzielle Anreize* zur Stärkung des internen Meldesystems sind denkbar[131]; die Prämienzahlung für Informanten ist in Deutschland jedoch bisher gesetzlich nicht vorgesehen.[132] Dieser Ansatz könnte aber das Risiko missbräuchlicher Meldungen erhöhen, da Mitarbeiter durch finanzielle Anreize motiviert werden, Informationen auch ohne eine zuverlässige Grundlage für ihre Anschuldigungen zu melden[133] oder selber einen Verstoß erzeugen[134]. Weiter besteht die Angst vor einer Förderung des Denunziantentums oder die Verschlechterung der Unternehmenskultur durch gegenseitige Überwachung und Unsicherheit.[135]

IV. Zentrale Konzernmeldestelle

§ 14 HinSchG regelt die *Organisationsformen interner Meldestellen*. Eine interne Meldestelle kann gem. § 14 Abs. 1 S. 1 HinSchG eine beim jeweiligen Beschäftigungsgeber oder bei der jeweiligen Organisationseinheit beschäftigte Person oder eine aus mehreren beschäftigten Personen bestehende Arbeitseinheit sein; es kann aber auch ein Dritter mit den Aufgaben einer internen Meldestelle betraut werden. § 14 Abs. 2 HinSchG erlaubt es mehreren privaten Beschäftigungsgebern mit 50 bis 249 Beschäftigten eine gemeinsame Stelle einzurichten und zu betreiben. Daneben gibt es keine spezielle Regelung für *konzernverbundene Unternehmen* im HinSchG. Allerdings zeigt der HinSchG-RegE in der Begründung zum § 14 Abs. 1 HinSchG die sog. Konzernlösung als Möglichkeit auf[136], welche auch der Rechtsausschuss des Deutschen Bundestages wegen ihrer hohen Praxisrelevanz in seiner Beschlussempfehlung[137] begrüßt. Mit der Konzernlösung[138] kann gemäß des

[129] Vgl. BT-Drs. 20/5992, S. 58; BT-Drs. 20/4909, S. 58; Dzida/Granetzny, 2020, S. 1203, 1205.
[130] Vgl. Dzida/Granetzny, 2020, S. 1203, Granetzny/Krause, 2020, S. 34.
[131] Vgl. Bundesrechtsanwaltskammer, 2022, S. 4; Bundesverband für Unternehmensjuristen, 2022, S. 8; Thüsig/Musiol, 2022, S. 2420; Dzida/Granetzny, 2020, S. 1203, 1206; Granetzny/Krause, 2020, S. 29; Schmolke, 2020, S. 11.
[132] Vgl. Dzida/Granetzny, 2020, S. 1206; Granetzny/Krause, 2020, S. 32.
[133] Vgl. Dzida/Granetzny, 2020, S. 1206.
[134] Vgl. Granetzny/Krause, 2020, S. 32.
[135] Vgl. Buchert, 2013, S. 145, 147; Fleischer/Schmolke, 2012, S. 364.
[136] Vgl. BT-Drs. 20/5992, S. 64f; Bundesregierung, 2023, FH zum HinSchG, S. 76f; Bundesregierung, 2022, RegE zum HinSchG, S. 91.
[137] Vgl. BT-Drs. 20/4909, S. 56.
[138] Vgl. BT-Drs. 20/4909, S. 56; Bundesregierung, 2023, FH zum HinSchG, S. 76f; Bundesregierung, 2022, RegE zum HinSchG, S. 91.

konzernrechtlichen Trennungsprinzips eine zentrale unabhängige und vertrauliche Stelle als Dritter im Sinne des § 14 Abs. 1 HinSchG agieren, der für mehrere selbstständige Unternehmen innerhalb des Konzerns stätig sein kann.[139]

Innerhalb größerer Konzerne ist ein *zentrales Hinweisgebersystem* für alle verbunden Unternehmen bereits seit mehreren Jahren Standard.[140] Die Möglichkeit zur Einrichtung einer zentralen Konzernmeldestelle wird befürwortet durch die Konzentration der Expertise und eine damit einhergehende schnelle sowie professionelle Fallbearbeitung, Nutzen von Synergien und Kostenersparnis durch die gemeinsame Nutzung von Ressourcen in Form von technischen Meldekanälen, Personal und Wissen bzw. Erfahrung sowie die zentrale und einheitliche Berichterstattung über relevante Hinweise an die Konzernleitung.[141] Bei global tätigen europäischen Konzernen bestehen Rechtspflichten der Konzerne in Drittländern, so könnte der Betrieb unverbundener dezentraler Meldesysteme womöglich mit den Anforderungen an Compliance-Systeme aus anderen Rechtsordnungen kollidieren.[142] Ebenfalls kann ein gemeinsames Konzernhinweisgebersystem den Schutz der Hinweisgebenden vor Vergeltungsmaßnahmen und somit das Schutzniveau erhöhen[143], da hinweisgebende Personen durch die größere Distanz einem geringeren Risiko von Repressalien ausgesetzt sind und innerhalb der Tochtergesellschaft die Gefahr der Offenlegung größer wäre. Zwar schreibt § 15 Abs. 1 HinSchG vor, dass für Meldungen zuständige Personen unparteiisch sein müssen. Allerdings kann innerhalb der lokalen Gesellschaft das Spannungsverhältnis an dieser Stelle größer sein als in der zentralen Konzernmeldestelle, wodurch das Vertrauen hinweisgebender Personen schwinden könnte.[144] Zentrale Meldestellen könnten mit größerer Unabhängigkeit, Objektivität und Professionalität agieren.[145] Weiter spricht für ein zentrales Hin-

[139] Vgl. Steinhauser/Saalwächter-Hirsch/Trouvain, 2023, S. 331; Bundesverband der Compliance Manager, 2022, S. 3, 5f.; Metzner/Hustert/Hommel, 2022, S. 118.
[140] Vgl. Deutscher Anwaltsverein, 2022, S. 28f; Gerdemann, 2022/1, S. 100f; Hamm-Düppe, 2022, S. 410; Metzner/Gloeckner, 2021, S. 256.
[141] Vgl. BT-Drs. 20/4909, S. 56; Bundesregierung, 2023, FH zum HinSchG, S. 76f; Bundesregierung, 2022, RegE zum HinSchG, S. 91; Bundesverband der Deutschen Industrie, 2022, S. 9f.; Bundesverband der Compliance Manager, 2022, 3, 5f.; Deutscher Anwaltsverein, 2022, S. 28f; Deutsches Institut für Compliance, 2022, S. 3; Gerdemann, 2022/1, S. 101; Hamm-Düppe, S. 410, Metzner/Hustert/Hommel, 2022, S. 118f; Zimmer/Humphrey, 2022, S. 374.
[142] Vgl. Deutsches Institut für Compliance, 2022, S. 4.
[143] Vgl. BT-Drs. 20/4909, S. 56; Bundesverband der Compliance Manager, 2022, S. 3, 5f.; Deutsches Institut für Compliance, 2022, S. 3; Gerdemann, 2022/1, S. 101.
[144] Vgl. Metzner/Glockner, 2021, S. 258.
[145] Vgl. Gerdemann, 2022/1, S. 100f; Metzner/Hommel, 2022, S. 119f.

weisgebersystem die Möglichkeit im Unternehmensverbund gezielt konzernweite Probleme und deren Ursachen festzustellen und wirksame Abhilfemaßnahmen ergreifen zu können.[146] Ein einheitliches Hinweisgeberschutzsystem erleichtert Kommunikations- und Trainingsmaßnahmen, ermöglicht einen einheitlichen Internetauftritt und stellt somit die Organisations- und Aufsichtspflichten der Unternehmensleitung sicher.[147] Nicht nur kennen Mitarbeiter, Führungskräfte, Mitbestimmungsgremien und externe Stakeholder bereits die möglichen Meldewege eines vorhandenen Hinweisgebersystem und haben schon umfassendes Vertrauen aufgebaut. Ein zentraler Meldekanal könnte auch sicherstellen, dass Hinweise externer Hinweisgebender ohne Wissen über interne Strukturen im richtigen Bereich verortet werden, die Risikoeinstufung des Hinweises einheitlich vorgenommen wird, die hinweisgebende Person – gerade bei landes- und geschäftsbereichsübergreifenden Sachverhalten – einen zentralen Ansprechpartner hätte und dass identische Hinweise nicht gleichzeitig bei verschiedenen Stellen bearbeitet werden und somit womöglich unterschiedliche Ergebnisse bei der Fallbearbeitung vermieden werden können.[148] Auch kann auf ein eingespieltes Beschwerdeverfahren mit vorhandenen Strukturen, Prozessen und Erfahrungen zurückgegriffen werden, wodurch prozessuale Schwierigkeiten und Verzögerungen gerade bei der Aufarbeitung gesellschaftsübergreifender Fälle minimiert werden könnten.[149] Bei der ausschließlichen Nutzung lokaler Meldekanäle könnten Informationen nicht vollständig weitergegeben werden, mehr Personen als notwendig in den Prozess eingebunden werden oder Untersuchungen unkoordiniert ablaufen. Ein konzernübergreifendes Hinweisgebersystem könnte unterstützen, gesetzlich zu berücksichtigende oder behördlich gesetzte Fristen besser einzuhalten und eine effektivere Bearbeitung von Hinweisen sicherstellen zu können. Auch könnte es eine Ungleichbehandlung ähnlicher Fälle minimieren und eine gewisse Einheitlichkeit gewährleisten.[150] Umgehen kann man mit dem zentralen Ansatz ebenfalls die Frage wie die Daten- und Informationsbeschaffung gerade hinsichtlich des Datenschutzrechts schnell und unkompliziert zwischen den Gesellschaften stattfin-

[146] Vgl. BT-Drs. 20/4909, S. 56; Gerdemann, 2022/1, S. 100f.
[147] Vgl. Hamm-Düppe, 2022, S. 411; Engels, 2020, S. 23.
[148] Vgl. Metzner/Hustert/Hommel, 2022, S. 118.
[149] Vgl. Hamm-Düppe, 2022, S. 410f; Metzner/Glockner, 2021, S. 259.
[150] Vgl. Metzner/Hustert/Hommel, 2022, S. 118; Metzner/Glockner, 2021, S. 259.

den darf oder unter welchen Umständen ein Hinweis ohne erneute Einbindung des Hinweisgebenden an die richtige bearbeitende Stelle abgegeben werden kann.[151] Nicht zuletzt gibt es Überschneidungen in den Anwendungsbereichen des HinSchG und des LkSG, die keinen Raum für unterschiedliche Beschwerdeverfahren lassen.[152]

Für den Einsatz *lokaler Hinweisgebersysteme* im Konzernverbund spricht in erster Linie die Abweichung vom zugrundeliegenden europäischen Recht. Gemäß Art. 8 Abs. 1 und Abs. 3 WBRL muss jedes Unternehmen mit mehr als 50 Mitarbeitern, unabhängig von einer Konzern- oder Gruppenzugehörigkeit, ein eigenes Hinweisgebersystem einführen und betreiben. Dabei erlaubt der Wortlaut des Art. 8 Abs. 6 WBRL nur eine gemeinsame Lösung für Unternehmen mit bis zu 249 Beschäftigten.[153] Es herrscht ein Dissens zwischen der deutschen Bundesregierung und der Europäischen Kommission darüber, ob andere Konzernunternehmen i.S.v. Art. 8 Abs. 5 WBRL als Dritte anzusehen sind. Diese Einschätzung der Bundesregierung wird teilweise deutlich kritisiert[154] und sogar als unionswidrig[155] eingestuft. Laut der Expertengruppe der EU-Kommission soll ein Konzernhinweisgebersystem zulässig sein, jedoch nur neben einem lokalen, auf Ebene der Tochtergesellschaften betriebenen System.[156] Die EU-Kommission vertritt die Meinung, dass jedes einzelne Gruppenunternehmen mit mindestens 50 Arbeitnehmern zur Einrichtung eines eigenen Meldekanals verpflichtet ist, da Art. 8 Abs. 3 WBRL keine Ausnahme für interne Meldungen innerhalb des Konzerns vorsehe und abschließend sei. Diese Einschätzung der EU-Kommission lässt sich lediglich in zwei Briefen finden, sodass hier ein informelles und extern zulasten der Unternehmen rechtlich unverbindliches Verwaltungshandeln einer Behörde vorliegt, welches bei der nationalen Auslegung zwar berücksichtigt, aber nicht zwingend befolgt werden muss[157], da es keine Rechtsquelle darstellt[158]. Alleine der EuGH besitzt gem. Art. 267 Abs. 1 AEUV das Auslegungsmonopol hinsichtlich des Unionsrechts.[159] Zwar vertritt Bürkle

[151] Vgl. Metzner/Hustert/Hommel, 2022, S. 118.
[152] Vgl. Hamm-Düppe, 2022, S. 410.
[153] Vgl. Metzner/Gloeckner, 2021, S. 256.
[154] Vgl. Dilling, 2022, S. 145; Kappen/Cho/Gärtner, 2022, S. 240; Nießen, 2022, S. 402.
[155] Vgl. Transparency International, 2022, S. 6.
[156] Vgl. Europäische Kommission, 2021, S. 2, Abschn. 3 a) (1), (2) und (3); Engels 2020, S. 22.
[157] Vgl. Bürkle, 2022, S. 336.
[158] Vgl. Leyens, 2015, S. 635.
[159] Vgl. Bürkle, 2022, S. 336.

mit seiner nach den Prüfkriterien des EuGH[160] vorgenommenen Beurteilung unter Berücksichtigung der grammatikalischen, systematischen und teleologischen Interpretation die Meinung, dass die WBRL den Betrieb einer einzigen zentralen Konzernmeldestelle zulässt und die gegenteilige Einschätzung der Europäischen Kommission bei genauer Betrachtung nicht überzeugen kann.[161] Fraglich bleibt aber, ob diese Interpretation der tatsächlichen Prüfung des EuGH standhält und ob für deutsche Unternehmen ein Risiko durch die Nichteinhaltung der WBRL bestehen könnte. Unter der Annahme, dass eine zentrale Konzernmeldestelle nicht europarechtskonform ist, könnte die Prüfung des Hinweises auch durch die Muttergesellschaft erfolgen, sofern die hinweisgebende Person über die Zugriffsmöglichkeit der zuständigen Stelle informiert wird und nicht widerspricht.[162] Dies könnte aber eine Umgehung des Vertraulichkeitsgebots gem. § 8 HinSchG darstellen, da die Identität der hinweisgebenden Person ohne ihre ausdrückliche Zustimmung keinen anderen Personen gegenüber offengelegt werden darf als den befugten Mitarbeitern. Zu Problemen könnte dies in der Praxis führen, wenn die hinweisgebende Person die Meldung an die Tochtergesellschaft vornimmt, einer Weitergabe der Meldung an die Muttergesellschaft aber widerspricht.[163] An dieser Stelle könnten auch datenschutzrechtliche Schadenersatzansprüche gem. Art. 82 Abs. 2 DSGVO, Geldbußen gem. Art. 83 Abs. 2 DSGVO i.V.m. § 43 BDSG und Freiheits- oder Geldstrafen gem. § 42 Art. 2, 3 BDSG auf das Unternehmen zukommen. Grund hierfür ist die Verarbeitung und Weitergabe von personenbezogenen Daten ohne Einwilligung der hinweisgebenden Person gem. Art. 6 lit. f DSGVO i.V.m. § 26 Abs. 1 S. 2 BDSG und Art. 6 lit. c DSGVO i.V.m. § 26 Abs. 1 S. 2 BDSG außerhalb der Entität, in der die hinweisgebende Person beschäftigt ist. Außerdem besteht in kleinen Unternehmen die Gefahr, dass trotz den Vorschriften zur Einhaltung der Vertraulichkeit, aufgrund der niedrigen Mitarbeiteranzahl oder aus mangelnder Kapazität durch die Anbindung der Hinweisbearbeitung an die Revision oder Personalabteilung (im Vergleich zu einer separaten Abteilung allein für die Annahme und Bearbeitung von Hinweisen in der Konzernmutter) Rück-

[160] Vgl. EuGH 6.10.2021 – C-561/19 (Consorzio) = EuZW 2022, S. 44, Rn. 42 ff.
[161] Vgl. Bürkle, 2022, S. 340.
[162] Vgl. Colneric, 2022, S. 2: Transparency International, 2022; S. 6f; Engels 2020, S. 22.
[163] Vgl. Metzner/Glockner, 2021, S. 257f. Engels, 2020, S. 23.

schlüsse auf die Identität der hinweisgebenden Person gezogen werden könnten.[164] Auch kann die Effektivität des Meldesystems nur durch die Nähe zur hinweisgebenden Person sichergestellt werden.[165] Eine sprachliche Hürde würde sich ebenfalls auf die Effektivität des internen Meldekanals auswirken und Hinweisgebende von Meldungen abhalten. Eine Herausforderung für die Mitarbeiter einer zentralen Meldestelle eines grenzübergreifend arbeitenden Konzerns, der lokale Gesellschaften in mehreren EU-Mitgliedsstaaten unterhält, könnten auch die verschiedenen nationalen Umsetzungen der WBRL darstellen.[166] Ebenso könnten im Rahmen der Hinweiskategorisierung und bei internen Untersuchungen spezifischen Kenntnisse über lokale Gegebenheiten von Vorteil sein.

Zwar sprechen aus Konzernsicht die besseren Argumente für ein zentrales Beschwerdeverfahren.[167] Ein möglicher Lösungsansatz für Konzerne könnte aber in der Kombination von zentralem und lokalem Hinweisgebersystem liegen. So könnte die Konzernmutter Prozessbeschreibungen und Verfahrensanweisungen zur Verfügung stellen, welche konzernweit auch in den Tochtergesellschaften Geltung finden sollen. Hinweise könnten sowohl zentral als auch lokal eingehen und zur weiteren Bearbeitung an die jeweilig zuständige Stelle gegeben werden – je nachdem ob lokales Spezialwissen benötigt wird oder nicht. Eine einfache und kostensparende Lösung könnte auch darin bestehen, dass alle zur Einrichtung von internen Meldestellen verpflichteten Konzerngesellschaften jeweils dieselbe unabhängige Ombudsperson als interne Meldestelle bestellen[168]; wichtig hierbei wäre aber das Beherrschen der jeweiligen Arbeitssprache der hinweisgebenden Personen. Sollte man sich ausschließlich für einen zentralen Meldekanal entscheiden, ist es gem. der Konzernlösung nach HinSchG-RegE notwendig, dass die originäre Verantwortung für die Weiterverfolgung und das Beheben eines festgestellten Verstoßes beim beauftragenden (lokalen) Unternehmen verbleibt. Ebenso müssen mit Blick auf mögliche Umsetzungsunterschiede in den einzelnen Ländern bei transnational tätigen Konzernen das Recht im jeweiligen Land des auftraggebenden Unternehmens beachtet werden. Weiter dürfen keine zu-

[164] Vgl. Metzner/Glockner, 2021, S. 258.
[165] Vgl. Europäische Kommission, 2021, S. 3; Engels, 2020, S. 23.
[166] Vgl. Steinhauser/Saalwächter-Hirsch/Trouvain, 2022, S. 331.
[167] Vgl. Hamm-Düppe, 2022, S. 410.
[168] Vgl. Dilling, 2022, S. 148.

sätzlichen Hürden für Hinweisgebende aufgebaut werden, so dass die Abgabe interne Meldungen in der im jeweiligen beauftragenden Konzernunternehmen vorherrschenden Arbeitssprache möglich sein muss. Ebenfalls ist bei der Hinweisbearbeitung durch eine zentrale Meldestelle eine Binnentrennung nach den jeweiligen Tochtergesellschaften zu gewährleisten.[169]

V. Anonyme Meldungen

Meldekanäle für interne Meldestellen müssen nach § 16 Abs. 1 S. 4f. des HinSchG[170] die *Möglichkeit der anonymen Meldung* und der darauffolgenden anonymen Kommunikation zwischen Meldestelle und Hinweisgebenden bereitstellen. Hervorzuheben ist an dieser Stelle, dass sich im HinSchG-RegE eine dahingehende Soll-Vorschrift findet[171], während der HinSchG-RefE lediglich eine Empfehlung beinhaltete[172]. Die Grundlage für diese Änderung lässt sich in Art. 6 Abs. 2 WBRL finden, welcher den Mitgliedsstaaten für die nationale Umsetzung einen Spielraum bei der Entscheidung, ob juristische Personen zur Entgegennahme und Weiterverfolgung anonymer Meldungen verpflichtet sind, ermöglicht.

Aus Compliance-Sicht ist die Pflicht zur Bearbeitung anonym eingehender Hinweise zu begrüßen. Die Möglichkeit der anonymen Hinweisgabe sollte für ein *effektives Hinweisgebersystem* unabdingbar sein, da die Meldebereitschaft potenzieller Hinweisgebender von der Möglichkeit zu anonymen Meldungen abhängen kann und durch ein solches Angebot eine potenzielle Hemmschwelle abgebaut werden könnte.[173] Allerdings ist die Möglichkeit einer anonymen Meldung nicht unumstritten. Durch sie könnte die Schwelle für die vorsätzliche Abgabe von falschen Meldungen abgebaut werden. Dadurch könnten Zweifel an der Glaubwürdigkeit anonymer Hinweise aufkommen, die Gefahr denunzierender Meldungen ansteigen und die Lauterkeit der Meldemotive in Frage gestellt werden, womit ein möglicher Meldemissbrauch einhergeht.[174] Daraus könnte eine mögliche Überlastung der

[169] Vgl. Steinhauser/Saalwächter-Hirsch/Trouvain, S. 331.
[170] Vgl. BT-Drs. 20/5992; S. 16; BT-Drs. 20/4909, S. 26.
[171] Vgl. BT-Drs. 20/5992; S. 16; BT-Drs. 20/4909, S. 26; Bundesregierung, 2023, FH zum HinSchG, S. 18; Bundesregierung, 2022, RegE zum HinSchG, S. 16.
[172] Vgl. Bundesministerium der Justiz, 2022, RefE zum HinSchG, S. 37, 87.
[173] Vgl. Steinhauser/Saalwächeter-Hirsch/Trouvain, 2023, S. 330; Bayreuther, 2022, S. 22; Bundesrechtsanwaltskammer, 2022, S. 5f; Bundesverband für Unternehmensjuristen, 2022, S. 6; Dilling, 2022, S. 148f; Lüneborg, 2022, S. 380f; Transparency International, 2022; S. 5f.; Dilling, 2021, S. 63; Colneric/Gerdemann, 2020, S. 137; Schmolke, 2020, S. 11; Taschke/Pielow/Volk, 2021, S. 91; Thüsig/Forst, 2021, § 6 Rz. 25, 65.
[174] Vgl. Steinhauser/Saalwächeter-Hirsch/Trouvain, 2023, S. 330; Dilling, 2022, S. 148; Colneric/Gerdemann, 2020, S. 135; Schmolke, 2020, S. 11; Council of Europe, 2014, S. 14, Rn. 12.

Meldestellen und damit verbunden eine Erhöhung der Personalkosten aufgrund des steigenden Bedarfs an Arbeitskraft in der internen Meldestelle ebenso wie die fehlende Möglichkeit zu Rückfragen an Hinweisgeber folgen.[175] Auch scheint es schwierig bei einer anonymen Meldung festzustellen, ob der persönliche Anwendungsbereich gem. § 1 HinSchG eröffnet ist, da möglicherweise keine Informationen zur hinweisgebenden Person in der Meldung genannt werden und diese womöglich erst in der nachfolgenden Kommunikation erfragt werden müssen. Weiter muss die notwendige Einrichtung technischer Vorrichtungen vorgenommen werden, mit der es zum einen möglich sein muss anonyme Hinweise zu erhalten und zum anderen mit anonymen Hinweisgebenden kommunizieren zu können. Dies geht genauso wie die Beauftragung von Ombudspersonen mit Kosten einher.[176] Betreffend die zuletzt genannten Punkte[177] kommt der Gesetzgeber den nach § 12 HinSchG zur Einrichtung interner Meldestellen verpflichteten Beschäftigungsgebern entgegen, indem er mit § 42 Abs. 2 HinSchG eine Übergangsregelung zum Inkrafttreten der Pflicht nach § 16 Abs. 1 S. 4 HinSchG geschaffen hat. Die Pflichten hinsichtlich anonymer Meldungen greifen somit erst ab 01.01.2025.

Ein weiterer Grund, welcher für die Zurverfügungstellung der Möglichkeit einer anonymen Hinweisgabe spricht, ist die *Legalitätspflicht*. Für den Vorstand kapitalmarktorientierter Gesellschaften dürfte sich bereits daraus ergeben auch anonymen Hinweisen zu möglichem rechtlichem Fehlverhalten nachgehen zu müssen, da nicht die Identität der Hinweisgebenden entscheidend ist, sondern der mögliche gemeldete Rechtsverstoß.[178] Ohne die Möglichkeit zu anonymen Meldungen gehen wesentliche Erkenntnisquellen verloren[179], wodurch wie bereits beschrieben die Effektivität der internen Meldekanäle sinken kann. Ein solches ineffektives Hinweisgebersystem stellt somit keine geeignete Aufsichtsmaßnahme i.S.v. § 130 Abs. 1 OWiG[180] oder (zukünftig) eine angemessene Vorkehrung zur Vermeidung und Aufdeckung

[175] Vgl. Steinhauser/Saalwächeter-Hirsch/Trouvain, 2023; Zimmer/Schwunk, 2022, S. 1172; Bundesministerium der Justiz und für Verbraucherschutz, 2020, S. 31.
[176] Vgl. Steinhauser/Saalwächeter-Hirsch/Trouvain, 2023, S. 330; Bundesministerium der Justiz, 2022, RefE zum HinSchG, S. 37; Lüneborg, 2022/2, S. 1273.
[177] Vgl. BT-Drs. 20/5992; S. 86f; BT-Drs. 20/4909, S. 61.
[178] Vgl. Dilling, 2022, S. 149; Freidank, 2022, S. 1872; Dilling, 2021, S. 63; Taschke, 2021, S. 86; Colneric/Gerdemann, 2020, S. 137; Schmolke, 2020, S. 11.
[179] Vgl. Bayreuther, 2022, S. 22; Dilling, 2022, S. 149.
[180] Vgl. Dilling, 2022, S. 149.

von Verbandstaten[181] dar. Anonyme Informationen sind nicht weniger relevant, sondern können umfangreicher und schonungsloser sein.[182] Für ein wirksames und funktionstüchtiges Hinweisgeberschutzsystem ist der Schutz des Hinweisgebers unerlässlich, durch die Entgegennahme anonymer Meldungen kann die Gefahr einer Repressalie von vornherein ausgeräumt werden.[183] Bei der Bußgeldbemessung ist laut Rechtsprechung ausdrücklich die Effektivität von Compliance-Maßnahmen zu berücksichtigen.[184] Die Möglichkeit zur anonymen Hinweisgabe ist also nicht nur nach dem HinSchG rechtskonform, sondern gilt nach anerkannten und branchenüblichen Maßstäben auch als Compliance-Maßnahme.

Ebenfalls gibt es einen Berührungspunkt zwischen der Möglichkeit zu anonymen Meldungen und dem *Verfahren bei internen Meldungen* gem. § 17 HinSchG. So stellt sich die Frage, wie eine anonyme Hinweisgabe mit der Pflicht der internen Meldestelle zur Eingangsbestätigung gem. § 17 Abs. 1 Nr. 1 HinSchG, zum Kontakterhalt mit der hinweisgebenden Person gem. § 17 Abs. 1 Nr. 3 HinSchG, zum Ersuchen für weitere Informationen gem. § 17 Abs. 1 Nr. 5 HinSchG und gem. § 17 Abs. 2 HinSchG für eine Rückmeldung an den Hinweisgebenden vereinbar ist. Die von der hinweisgebenden Person gewählte Anonymität könnte als konkludenter Verzicht auf Unterrichtung bzw. Kontaktaufnahme verstanden oder diese schon denklogisch ausgeschlossen werden.[185] Bei den genannten Kontaktaufnahmen gem. § 17 Abs. 1 HinSchG müssten juristische Personen eine Ombudsperson einschalten oder die technische Lösung eines web-basierten Meldekanal implementieren, der eine Follow-up-Kommunikation mit Hinweisgebenden unter Wahrung der Anonymität ermöglicht, damit diese eine Bestätigung und Rückmeldung erhalten können und um Rückfragen der untersuchenden Stelle zu ermöglichen.[186] Wird der interne Meldekanal in Form einer web-basierten Lösung gewählt, muss bei der Einführung und Ausgestaltung des Verfahrens bei internen Meldungen der Betriebsrat gem. § 17 HinSchG i.V.m. § 87 Abs. 1 Nr. 1, Nr. 6 BetrVG einbezogen werden, da die technische

[181] Vgl. Bundesregierung, 2020, RegE zum VerSanG, § 3 Abs. 1 Nr. 2 VerSanG-RegE, S. 8; § 15 Abs. 1 Nr. 6 und 7 VerSanG-RegE, S. 13.
[182] Vgl. Zimmer/Schwunk, 2022, S. 1172.
[183] Vgl. Zimmer/Schwunk, 2022, S. 1172; Dohrmann, 2021, S. 331.
[184] Vgl. BGH, Urt. v. 09.05.2017 – 1 StR 265/16 (Panzerhaubitze) = BeckRS 2017, 114578, Rz. 118.
[185] Vgl. Taschke/Pielow/Volk, 2021, S. 90; Thüsig/Rombey, 2018, S. 1004.
[186] Vgl. Dilling, 2022, S. 149; Taschke/Pielow/Volk, 2021, S. 90; Colneric/Gerdemann, 2020, S. 137.

Einrichtung geeignet ist das Verhalten oder die Leistung der Arbeitnehmenden zu überwachen.

Gemäß des *Vertraulichkeitsgebotes* (weitere Ausführungen in Kapitel VII. Repressalienverbot und Beweislastumkehr) aus § 8 Abs. 1 Nr. 1 HinSchG haben Meldestellen auch die Vertraulichkeit der Identität anonymer hinweisgebender Personen zu wahren. In diesem Zusammenhang müssen *datenschutzrechtliche Vorschriften* Beachtung finden. Durch die Pflicht zur Berücksichtigung der DSGVO und des BDSG gem. § 10 HinSchG können datenschutzrechtliche Einschränkungen auf Seiten der betroffenen Person der Vertraulichkeit der Identität des anonymen Hinweisgebers entgegenstehen.[187] Nach Art. 14 Abs. 1, Abs. 3 lit. a DSGVO muss eine von der Datenverarbeitung betroffene Person innerhalb eines Monats über die Quelle, aus der die Daten stammen, informiert werden. So müsste die vom Hinweis betroffene Person spätestens einen Monat nach der Meldung über die Identität des Hinweisgebers informiert werden. Art. 15 lit. g DSGVO definiert u. a. ein Recht auf Information über die Herkunft der personenbezogenen Daten, wonach die vom Hinweis betroffene Person ein Recht darauf haben kann, die Identität des Hinweisgebers zu erfahren. Nach Art. 23 Abs. 1 DSGVO könnten diese Pflichten und Rechte unter bestimmten Voraussetzungen durch Rechtsvorschriften beschränkt werden. Ein Risiko besteht für das Unternehmen hier in Form möglicher datenschutzrechtlicher Schadenersatzansprüche gem. Art. 82 Abs. 2 DSGVO, Geldbußen gem. Art. 83 Abs. 2 DSGVO i.V.m. § 43 BDSG oder Freiheits- oder Geldstrafen gem. § 42 Art. 2, 3 BDSG.

VI. Schutzvoraussetzungen

Hinweisgebende Personen müssen die die Voraussetzungen des § 33 HinSchG erfüllen, um Zugang zu den Schutzmaßnahmen der §§ 35 bis 37 HinSchG zu erhalten. Die hinweisgebende Person muss gem. § 33 Abs. 1 Nr. 2 HinSchG zum Zeitpunkt der Meldung oder Offenlegung hinreichenden Grund zur Annahme gehabt haben, dass die von ihr gemeldeten oder offengelegten Informationen der Wahrheit entsprechen. Weiter müssen die Informationen gem. § 33 Abs. 1 Nr. 3 HinSchG Verstöße betreffen, die in den Anwendungsbereich des HinSchG fallen, oder die hinweisgebende Person zum Zeitpunkt der Meldung oder Offenlegung hinreichenden Grund zu der

[187] Vgl. Altenbach/Dierkes, 2020, S.128ff; Dzida/Granetzny, 2020, S. 1205f.

Annahme gehabt haben, dass dies der Fall sei. Nicht geschützt werden grundlose Spekulationen oder leichtfertige Meldungen ohne ein zumutbares Bemühen nach Verifizierung; es müssen tatsächliche Anhaltspunkte für einen Verstoß vorliegen.[188] Im HinSchG wurden die unbestimmten Rechtsbegriffe aus der deutschen Fassung der WBRL übernommen. Sinnvoll wäre es an dieser Stelle gewesen an die bekannten Verschuldensmaßstäbe von Vorsatz und Fahrlässigkeit anzuknüpfen, wodurch man eine höhere Rechtssicherheit herbeiführen und eine Konsistenz mit der Schadensersatzregelung in § 37 HinSchG gewährleisten könnte.[189] Ebenfalls hätte hier die Motivation der hinweisgebenden Person angemessen berücksichtigt werden können.[190] Weiter wäre eine Bereinigung der Widersprüche in § 33 Abs. 1 HinSchG sinnvoll[191], da einerseits die subjektiven Beweggründe für das Vorliegen eines hinreichenden Grundes zur Wahrheitsannahme keine Rolle spielen dürfen[192], da es sich um eine ex-ante Betrachtung eines objektiven Dritten handelt[193]. Andererseits werden aber die missbräuchliche oder böswillige Meldung von unrichtigen Informationen nicht geschützt.[194] Es dürfen keine überhöhten Anforderungen an die Überprüfung des Wahrheitsgehalts der Meldung gestellt werden.[195] Allerdings könnte für hinweisgebende Personen eine Schwierigkeit darin bestehen abzusichern, dass sie gutgläubig handeln. Selbst wenn die hinweisgebende Person subjektiv und objektiv gutgläubig ist, besteht die Gefahr, dass eine von der Meldung oder Offenlegung betroffene Person das anders sieht und den Hinweisgebenden dem Schutzbereich des HinSchG zu entziehen versucht.[196] Dies könnte wiederum dazu führen, dass potenzielle hinweisgebende Personen vor einer Meldung zurückschrecken. Die Häufung von wissentlichen Falschmeldungen und eine Überflutung der Meldekanäle dürfte sich in Grenzen halten, da bei einer vorsätzlichen oder grob fahrlässigen Falschmeldung nicht nur der Schutz vor Repressalien entfällt, sondern die hinweisgebende Person nach § 38 HinSchG zum Schadenersatz verpflichtet ist.

[188] Vgl. BT-Drs. 20/3442, S. 92.
[189] Vgl. Deutsches Institut für Compliance, 2022, S. 2; Gerdemann, 2021; S. 39.
[190] Vgl. Deutsches Institut für Compliance, 2022, S.2.
[191] Vgl. Deutsches Institut für Compliance, 2022, S.2.
[192] Vgl. BT-Drs. 20/3442, S. 92.
[193] Vgl. Steinhauser/Saalwächter-Hirsch/Trouvain, 2022, S. 332.
[194] Vgl. BT-Drs. 20/3442, S. 100.
[195] Vgl. Steinhauser/Saalwächter-Hirsch/Trouvain, 2022, S. 332.
[196] Vgl. Dilling, 2019, S. 216.

Ebenfalls sind die *Voraussetzungen für den Schutz verbundener natürlicher Personen* zu erwähnen. Die in § 34 Abs. 1 HinSchG genannten unterstützenden Personen sind geschützt, sofern die gemeldeten oder offengelegten Informationen gem. § 34 Abs. 1 Nr. 1 HinSchG zutreffend sind oder die unterstützende Person zum Zeitpunkt der Unterstützung hinreichenden Grund zu der Annahme hatte, dass die von der hinweisgebenden Person gemeldeten oder offengelegten Informationen der Wahrheit entsprachen, und wenn gem. § 34 Abs. 1 Nr. 2 HinSchG Verstöße betroffen sind, die in den Anwendungsbereich dieses Gesetzes fallen, oder die unterstützende Person zum Zeitpunkt der Unterstützung hinreichenden Grund zu der Annahme hatte, dass dies der Fall sei. Die Voraussetzungen zum Schutz der hinweisgebenden Person gem. § 33 HinSchG müssen dem Wortlaut nach also gerade nicht vorliegen. Der Schutz der mit der hinweisgebenden Person in Verbindung stehenden Personen gem. § 34 Abs. 2 Nr. 1 HinSchG erfordert dahingegen das Erfüllen der Voraussetzungen des § 33 HinSchG durch die hinweisgebende Person. Auffällig ist hier der unterschiedliche Umgang mit der Abhängigkeit von der Schutzwürdigkeit der hinweisgebenden Personen. Was für eine solche Abhängigkeit spricht ist die nicht vorhandene Möglichkeit einer Meldung oder Offenlegung durch eine verbundene Person.[197] Weiter sprechen das Ziel der zugrunde liegenden WBRL für eine Abhängigkeit des Schutzes, was die Förderung allein berechtigten Whistleblowings einschließt.[198] Beide Regelungen sind thematisch nicht beim persönlichen Anwendungsbereich des HinSchG in § 1 positioniert, was gegen die Abhängigkeit des Schutzes beider Personengruppen von der Schutzwürdigkeit der hinweisgebenden Person spricht.[199] Auch fällt auf, dass verschieden mit dem Vorliegen einer hinreichend begründeten Annahme des Vorliegens der Wahrheit der verbundenen Person umgegangen wird. Nur bei den nach § 34 Abs. 1 HinSchG muss gem. Nr. 1 ein solches vorliegen. Gegen das Vorliegen spricht hingegen, dass relevante Informationen nicht vorliegen könnten oder es der Person nicht mög-

[197] Vgl. Siemes, 2022, S. 10; Forst, 2020, S. 298; a. A. Fest in Franzen/Gallner/Oetker, 2022, RL (EU) 2019/1937, Art. 21, Rn. 5.
[198] Vgl. Fest in Franzen/Gallner/Oetker, 2022, RL (EU) 2019/1937, Art. 1, Rn. 48, 51f; Art. 4 Rn. 1 Art. 19, Rn. 16; Siemes, 2022, S. 11; 2021, S. 51.
[199] Vgl. Fest in Franzen/Gallner/Oetker, 2022, RL (EU) 2019/1937, Art. 4, Rn. 24; Art. 6, Rn. 36; Art. 21, Rn. 28; Siemes, 2022, S. 10f; Siemes, 2021, S. 99.

lich ist eine vollumfassende Beurteilung im Hinblick auf die enthüllten Informationen vorzunehmen.[200] Ebenso sei das Handeln eines bösgläubigen Whistleblowers einem gutgläubigen Dritten objektiv nicht zuzurechnen.[201]

VII. Repressalienverbot und Beweislastumkehr

Sowohl gegen hinweisgebende Personen gerichtete *Repressalien* als auch die Androhung und der Versuch Repressalien auszuüben sind gem. § 36 Abs. 1 HinSchG verboten. Definiert werden Repressalien in § 3 Abs. 6 HinSchG als Handlungen oder Unterlassungen im Zusammenhang mit der beruflichen Tätigkeit, die eine Reaktion auf eine Meldung oder eine Offenlegung sind und durch die der hinweisgebenden Person ein ungerechtfertigter Nachteil entsteht oder entstehen kann. Weder wird der *Begriff Repressalie* im Gesetzestext weiter erläutert noch werden Beispiele genannt.[202] Art. 19 WBRL leistete wertvolle Hilfestellung und zählte 15 nicht abschließende Fallgruppen von beispielhaften Repressalien gegen hinweisgebende Personen auf.[203] Fraglich ist, warum dem Rechtsanwender im Gesetzestext des HinSchG Beispiele vorenthalten werden. Dass der Begriff einer Erläuterung bedarf, scheint dem Entwurfsverfasser klar gewesen zu sein, da in der Entwurfsbegründung an fünf Stellen verschiedene anschauliche Beispiele aus dem Katalog des Art. 19 WBRL genannt werden.[204] Beispiele würden Unternehmen und hinweisgebenden Personen gleichermaßen bei der Einschätzung, welche Verhaltensweisen verboten sind, unterstützen.[205] Ein hoher Detaillierungsgrad könnte die effektive Durchsetzung des Verbots von Repressalien fördern.[206] Auf Unternehmen könnten durch Unwissenheit darüber, was genau unter den Begriff Repressalie fällt, Geldstrafen gem. § 40 Abs. 2 Nr. 3 HinSchG zukommen.

Der *Beweislastumkehr* gem. § 36 Abs. 2 S. 1 HinSchG nach wird zeitlich unbefristet vermutet, dass eine nach Meldung oder Offenlegung erfolgte Benachteiligung gegen das Verbot von Repressalien aus § 36 Abs. 1 HinSchG verstößt. Die Begründung dafür liegt darin, dass hinweisgebende Personen nicht von vornherein von einer Meldung oder Offenlegung eines Verstoßes

[200] Vgl. Fest in Franzen/Gallner/Oetker, 2022, RL (EU) 2019/1937, Art. 6, Rn. 10ff; Forst, 2020, S. 298; Siemes, 2022, S. 11.
[201] Vgl. Forst, 2020, S. 297f; Siemes, 2020, S. 10.
[202] Vgl. Dilling, 2022, S. 150; Zimmer/Schwunk, 2022, S. 1168; Gerdemann, 2021; S. 38.
[203] Vgl. Colneric, 2022, S. 4; Dilling, 2022, S. 150; Colneric/Gerdemann, 2020, S. 109; Schmolke, 2020, S. 5.
[204] Vgl. BT-Drs. 20/5992; S. 2, 29, 32, 34f, 81; Bundesregierung, 2023, FH zum HinSchG, S. 2, 33, 37; 40, 97f; Bundesregierung, 2022, RegE zum HinSchG, S. 2; 31, 35, 37, 110.
[205] Vgl. Dilling, 2022, S. 150.
[206] Vgl. Colneric/Gerdemann, 2020, S. 109.

durch die schwierige Beweisführung im Prozess abgeschreckt und die Möglichkeit ihre Rechte geltend zu machen erleichtert werden sollen.[207] Der hinweisgebenden Person, die eine Benachteiligung erleidet, ist es oft nicht möglich den kausalen Zusammenhang zwischen Meldung oder Offenlegung und Benachteiligung nachzuweisen. Die hinweisgebende Person ist nicht komplett frei von einer Beweislast. So muss sie darlegen und beweisen, dass eine Maßnahme eine Benachteiligung darstellt.[208] Dies könnte zu einer Abschreckung potenzieller hinweisgebender Personen führen, was wiederum die Effektivität des Hinweisgebersystems einschränken kann. Eine Klarstellung zu den Beweispflichten der hinweisgebenden Person wäre sinnvoll.[209] Im Gegensatz zur hinweisgebenden Person stehen dem Beschäftigungsgeber alle Unterlagen und Informationen zur Verfügung, welche die Grundlage für die ergriffenen Maßnahmen waren; aufgrund des Informationsungleichgewichts ist es sach- und interessengerecht dieser Partei die Beweislast aufzuerlegen.[210] Nach § 36 Abs. 2 S. 2 HinSchG kann eine Vermutung widerlegt werden, wenn die Benachteiligung auf hinreichend gerechtfertigten anderen Gründen oder nicht auf der Meldung oder Offenlegung basierte. Man unterscheidet also zwei Tatbestandsmerkmale der Repressalie: die kausale Verknüpfung der Maßnahme mit der Meldung oder Offenlegung und das Vorliegen oder die Möglichkeit eines ungerechtfertigten Nachteils.[211] Als Beispiele nennt der HinSchG-RegE betriebsbedingte Gründe und Fehlverhalten der hinweisgebenden Person und die Beteiligung der hinweisgebenden Person am gemeldeten Verstoß.[212] Dies könnte einen abschreckenden Effekt auf potenzielle Hinweisgeber aus dem Täterkreis haben. Diese Informationen sind aber für das Unternehmen und die Effektivität des Hinweisgebersystems gleichermaßen wichtig, da diese Personen häufig die größte Kenntnis besitzen und zur Aufklärung beitragen könnten.[213]

Problematisch ist für Unternehmen eine Widerlegung bei Vorliegen von *Motivbündeln*; wenn also die Hinweisgabe zwar einer mehrerer Faktoren für die

[207] Vgl. BT-Drs. 20/5992; S. 81f; Bundesregierung, 2023, FH zum HinSchG, S. 98f; Bundesregierung, 2022, RegE zum HinSchG, S. 111.
[208] Vgl. Steinhauser/Saalwächter-Hirsch/Trouvain, 2022, S. 332.
[209] Vgl. Deutsches Institut für Compliance, 2022, S.7.
[210] Vgl. BT-Drs. 20/5992; S. 81f; Bundesregierung, 2023, FH zum HinSchG, S. 98f; Bundesregierung, 2022, RegE zum HinSchG, S. 111.
[211] Vgl. Zimmer/Schwunk, 2022, S. 1168.
[212] Vgl. BT-Drs. 20/5992; S. 81f; Bundesregierung, 2023, FH zum HinSchG, S. 98f; Bundesregierung, 2022, RegE zum HinSchG, S. 112.
[213] Vgl. Zimmer/Schwunk, 2022, S. 1168.

veranlasste Benachteiligung war, daneben aber ein rechtfertiger Grund vorliegt.[214] Der Gesetzgeber erfordert an dieser Stelle nur, dass die Meldung oder Offenlegung nicht das vorherrschende Motiv war.[215]

Auch ist unklar, wann die *Vermutungswirkung für die Kausalität* widerlegt werden kann und ob eine trennscharfe Differenzierung zwischen den beiden Tatbestandsmerkmalen der Beweislastumkehr überhaupt möglich ist.[216] Wenn für die Benachteiligung ein bestimmter rechtfertigender Grund vorliegt, ist die Kausalität zu verneinen, da die Maßnahme nicht auf der Meldung, sondern auf dem Rechtsfertigungsgrund beruht. Die Kausalität hat somit nur eine eigene Bedeutung, wenn nicht schon ein berechtigter Grund vorliegt[217]; wann ihre Widerlegung möglich ist, wird nicht erläutert. Zu berücksichtigen sein soll aber der zeitliche Zusammenhang zwischen Meldung oder Offenlegung und Benachteiligung.[218] Vermuten lässt sich, dass man die Kausalität am einfachsten damit widerlegen kann, dass die Handlungen vornehmende Partei keine Kenntnis von der Meldung oder Offenlegung der hinweisgebenden Person hatte.[219] Um einen Nachweis gegen die Kausalität der Benachteiligung zu erbringen, sollten Entscheidungen, die Repressalien darstellen könnten, von Personen ohne Kenntnis der Meldung getroffen werden.[220] Zur Widerlegung der fehlenden Rechtfertigung empfiehlt sich für Beschäftigungsgeber eine umfassende Dokumentation der Meldung gem. § 11 HinSchG sowie der ergriffenen Folgemaßnahmen ebenso wie eine genaue Aufzeichnung der Mitarbeiterbewertung, Bonussysteme, Karriereentwicklungen, erteilter Abmahnungen sowie bereits aufgetretener Probleme und Konflikte.[221] Die Meldung eines potenziellen Verstoßes kann durch die Beweislastumkehr für den Arbeitnehmer einen faktischen Kündigungsschutz bewirken[222], da bisher die Darlegungs- und Beweislast hinsichtlich des Kausalzusammenhangs zwischen zulässiger Rechtsausübung des Arbeitnehmers und unzulässiger Maßregelung durch den Arbeitgeber beim allgemeinen

[214] Vgl. Gerdemann, 2022/2; S. 8; Zimmer/Schwunk, 2022, S. 1168.
[215] Vgl. BT-Drs. 20/5992; S. 83; Bundesregierung, 2023, FH zum HinSchG, S. 100; Bundesregierung, 2022, RegE zum HinSchG, S. 113.
[216] Vgl. Zimmer/Schwunk, 2022, S. 1168f.
[217] Vgl. Zimmer/Schwunk, 2022, S. 1169.
[218] Vgl. BT-Drs. 20/5992; S. 82f; Bundesregierung, 2023, FH zum HinSchG, S. 99f; Bundesregierung, 2022, RegE zum HinSchG, S. 112.
[219] Vgl. Zimmer/Schwunk, 2022, S. 1169.
[220] Vgl. BT-Drs. 20/5992; S. 82f; Bundesregierung, 2023, FH zum HinSchG, S. 99f; Bundesregierung, 2022, RegE zum HinSchG, S. 112.; Zimmer/Schwunk, 2022 S. 1171.
[221] Vgl. Bundesrechtsanwaltskammer, 2022, S. 9; Degenhart/Dziuba, 2021, S. 570, 574; Dohrmann, 2021, S. 331; Dzida/Granetzny, 2020, S. 1204.
[222] Vgl. Fuhlrott/Henckel, 2022, S. 444; Degenhart/Dziuba, 2021, S. 570, 573; Dohrmann, 2021, S. 331; Dzida/Granetzny, 2020, S. 1204.

Maßregelungsverbot des § 612 a BGB dem Arbeitnehmer oblag[223]. Weiter muss der Arbeitgeber nun bei Kündigungen hinweisgebender Personen innerhalb der Probezeit die Gründe der Kündigung nachweisen, obwohl eine rechtliche Begründung zur Notwendigkeit bisher nicht bestand.[224] Somit könnte die betriebliche Entscheidungsfreiheit eingeschränkt werden.

Bei einem Verstoß gegen das Verbot von Repressalien haben hinweisgebende Personen gegen den Verursacher einen *Schadensersatzanspruch* gem. § 37 Abs. 1 HinSchG. Gem. § 37 Abs. 2 HinSchG besteht allerdings kein Anspruch auf die Begründung eines Beschäftigungsverhältnisses oder auf einen beruflichen Aufstieg. Fraglich ist, ob sich die Beweislast auch auf die Rechtsfolgenseite bezieht – also darauf, dass aufgrund des Verstoßes gegen das Repressalienverbot ein Schaden entstanden ist. Der Wortlaut des § 36 Abs. 2 HinSchG bezieht sich explizit nur auf die beiden Tatbestandsmerkmale der Repressalie und nicht auf sonstige Folgeansprüche, wodurch davon auszugehen ist, dass die Beweislast nicht für die Rechtsfolgenseite gilt.[225] Folglich hat die hinweisgebende Person darzulegen, dass ihm wegen einer Repressalie ein Schaden entstanden ist. Beispielsweise müsste er also darlegen, dass er nicht zum nächstmöglichen Termin ordentlich gekündigt oder ein befristetes in ein unbefristetes Arbeitsverhältnis umgewandelt worden wäre. Trotzdem wäre es sinnvoll, dass der Arbeitgeber Argumente wie betriebliche Gründe dafür anführen kann, warum keine berechtigte Erwartung des Arbeitnehmers bspw. auf Umwandlung, Verlängerung, Nicht-Kündigung bestanden haben konnte. Auch im Rahmen von *Schmerzensgeldansprüchen* ist die Beweislastumkehr stets anwendbar[226], da in § 37 Abs. 1 S. 2 HinSchG aufgeführt wird, dass die hinweisgebende Person wegen eines Schadens, der nicht Vermögensschaden ist, eine angemessene Entschädigung in Geld verlangen kann. Allerdings ist der Nachweis einer Verletzung der in § 253 Abs. 2 BGB genannten Rechtsgüter oftmals schwer, da Repressalien vielschichte Erscheinungsformen einnehmen können – bspw. bei psychischen Belastungen.[227] Wäre ein Schadensersatz- und Schmerzensgeldan-

[223] Vgl. BAG Urt. V. 18.10.2017 – 10 AZR 330/16, NZA 2017, 1452, 1456 Rn. 42; Dohrmann, 2021, S. 331; ErfK/Preis, 2021, §612a BGB, Rn. 22; Dzida/Granetzny, 2020, S. 1201, 1204.
[224] Vgl. Bundesrechtsanwaltskammer, 2022, S. 9; Degenhart/Dziuba, 2021, S. 570, 573; Dohrmann, 2021, S. 331.
[225] Vgl. Zimmer/Schwunk, 2022, S. 1169.
[226] Vgl. Zimmer/Schwunk, 2022, S. 1170.
[227] Vgl. Steinhauser/Saalwächter-Hirsch/Trouvain, 2022, S. 333; Zimmer/Schwunk, 2022, S. 1170.

spruch jedoch nicht möglich, würde das Vertrauen der hinweisgebenden Personen minimiert werden und somit die Effektivität des Hinweisgebersystems senken.

Auch sollte die Möglichkeit *zeitlicher Einschränkungen* beim Repressalienverbot und der Beweislastumkehr diskutiert werden.[228] So ist zu klären, ob die Beweislastumkehr zeitlich beschränkt ist; wieviel Zeit also nach der Meldung oder Offenlegung vergangen sein muss, damit eine nachteilige Maßnahme oder Unterlassen aufgrund des § 36 Abs. 2 HinSchG als Repressalie gilt.[229] Der Wortlaut ist unbestimmt und erfordert nur, dass die Benachteiligung nach der Meldung oder Offenlegung erlitten werden muss. ErwG 44 der WBRL fordert nur einen engen Zusammenhang zwischen Meldung und erlittener Benachteiligung. Für den Arbeitgeber wird es bei fortschreitendem Zeitablauf einfacher sein die Vermutungswirkung zu widerlegen.[230] Eine klar definierte zeitliche Grenze wäre hier sinnvoll.[231] Am zweckmäßigsten scheint ein Gleichlauf mit der dreijährigen Löschfrist des § 11 Abs. 5 HinSchG zu sein, um die verschiedenen Interessenlagen in einen angemessenen Ausgleich zu bringen.[232] Weiter stellt sich die Frage wie lange sich der Arbeitnehmer auf den Verstoß gegen das Repressalienverbot berufen kann. Da sich hierzu keine Regelung im Gesetzestext finden lässt, ist auf die Regelverjährungsfrist von drei Jahren gem. § 195 BGB zurückzugreifen.[233] Dieser Ansatz stünde im Einklang mit der dreijährigen Löschfrist des § 11 Abs. 5 HinSchG. Zu praktischen Problemen für Unternehmen könnte ein längerer Zeitraum führen, da nach Löschung aller Daten auf Arbeitgeberseite kein Informationsüberschuss mehr vorliegt. Ein Konfliktpotenzial birgt auch die datenschutzrechtliche Löschungsverpflichtung aus Art. 17 Abs. 1 lit. a DSGVO. Personenbezogene Daten sollen nach Ansicht der deutschen Datenschutzbeauftragten und des Europäischen Datenschutzbeauftragten grundsätzlich spätestens zwei Monate nach Abschluss der Untersuchung gelöscht werden, wenn nicht die Klärung erforderlicher weiterer rechtlicher Schritte wie Disziplinarverfahren oder die Einleitung von Strafverfahren im

[228] Vgl. Deutsches Institut für Compliance, 2022, S.7; Zimmer/Schwunk, 2022, S. 1170.
[229] Vgl. Zimmer/Schwunk, 2022, S. 1170.
[230] Vgl. Dilling, 2019, S. 214, 219; Dilling, 2021, S. 60, 65; Dohrmann, 2021, S. 331.
[231] Vgl. Bundesrechtsanwaltskammer, 2022, S. 10; Bundesverband für Unternehmensjuristen, 2022, S. 8; Deutscher Anwaltsverein, 2022, S. 30f; Deutsches Institut für Compliance, 2022, S.6f.
[232] Vgl. Bundesverband der Deutschen Industrie, 2022, S. 8; Bundesverband für Unternehmensjuristen, 2022, S. 8; Deutsches Institut für Compliance, 2022, S. 35; Zimmer/Schwunk, 2022, S 1171.
[233] Vgl. Bundesverband der Compliance Manager, 2022, S. 7; Bundesverband für Unternehmensjuristen, 2022, S. 4; Deutsches Institut für Compliance, 2022, S. 35; Zimmer/Schwunk, 2022, S 1171.

Raum steht.[234] Diese Ausnahme nach Art. 17 Abs. 3 lit. e DSGVO soll die Geltendmachung eigener Rechtsansprüche sowie die Verteidigung gegen Rechtsansprüche Dritter sichern, indem ein einseitig benachteiligendes Beweismitteldefizit infolge der Löschungsverpflichtung verhindert wird.[235] Wenn die Wahrscheinlichkeit der Geltendmachung von Rechtsansprüchen oder deren Gewicht dem mit der Speicherung verbundenen Eingriff in die Grundrechte des Betroffenen überwiegt, dürfen Daten länger aufbewahrt werden.[236] Bei Verstoß gegen die DSGVO können für den Arbeitgeber datenschutzrechtliche Schadenersatzansprüche gem. Art. 82 Abs. 2 DSGVO, Geldbußen gem. Art. 83 Abs. 2 DSGVO i.V.m. § 43 BDSG und Freiheits- oder Geldstrafen gem. § 42 Art. 2, 3 BDSG. Sollten die Unternehmen die Daten bereits gelöscht haben, hat es nur noch wenige Möglichkeiten zur Entkräftung der Behauptung des Arbeitnehmers, wodurch auch ein Imageschaden entstehen kann.[237]

VIII. Ausnahmen vom Vertraulichkeitsgebot

Gemäß des *Vertraulichkeitsgebotes* aus § 8 Abs. 1 Nr. 1 HinSchG haben Meldestellen die Vertraulichkeit der Identität hinweisgebender Personen zu wahren, sofern die Meldung in den sachlichen Anwendungsbereich fällt oder die hinweisgebende Person zum Zeitpunkt der Meldung hinreichenden Grund zur Annahme hatte, dass dies der Fall sei. Gem. § 8 Abs. 1 Nr. 2 und Nr. 3 HinSchG ist ebenso die Vertraulichkeit der Identität von Personen, die Gegenstand einer Meldung sind, und der sonstigen in der Meldung genannten Personen zu wahren. So muss also auch eine interne Meldestelle die ihr bekannte Identität hinweisgebender und betroffener Person schützen und darf diese nicht ohne Weiteres Dritten bekannt geben. Bereits Art. 16 Abs. 2 und Abs. 3 WBRL sehen weitreichende *Ausnahmen* vom Vertraulichkeitsgebot vor, im HinSchG werden diese in § 9 geregelt. Bedenklich ist hierbei, dass § 9 HinSchG zum Teil über die Ausnahmen der WBRL hinausgeht und somit die Vertraulichkeit der Identität nicht umfassend geschützt wird.[238]

[234] Vgl. Datenschutzkonferenz, 2018, S. 11; Europäischer Datenschutzbeauftragter, 2016, S. 9, Rn. 29.
[235] Vgl. Altenbach/Dierkes, 2020, S. 130.
[236] Vgl. Simitis/Hornung/Spiecker gen. Döhmann/Dix, 2019, Art. 17 DSGVO, Rn. 38.
[237] Vgl. Altenbach/Dierkes, 2020, S. 130.
[238] Vgl. Dilling, 2022, S. 147; Transparency International, 2022; S. 3.

So sieht Art. 16 Abs. 2 WBRL vor, dass Informationen nur dann offengelegt werden dürfen, wenn nach Unionsrecht oder nationalem Recht eine notwendige und verhältnismäßige Pflicht im Rahmen von *Untersuchungen durch nationale Behörden oder Gerichtsverfahre*n darstellt; ein einfaches Verlangen einer Strafverfolgungsbehörde darf das Vertraulichkeitsgebot demnach nicht entfallen lassen.[239] Umgesetzt wird Art. 16 Abs. 2 WBRL in § 9 Abs. 2 Nr. 1 HinSchG[240], wonach Informationen über die Identität einer hinweisgebenden Person in Strafverfahren auf Verlangen der Strafverfolgungsbehörden weitergegeben werden dürfen; Notwendigkeit und Verhältnismäßigkeit werden an dieser Stelle im Normtext nicht genannt. In der Entwurfsentscheidung heißt es, § 9 Abs. 2 HinSchG regele grundsätzlich nur die Befugnis der Meldestellen Daten zur Identität der hinweisgebenden Person weiterzugeben. Die Verpflichtung zur Herausgabe dieser Daten ergebe sich aus den allgemeinen Gesetzen wie etwa der StPO. § 4 Abs. 4 HinSchG eröffne die Anwendung des Strafprozessrechts, wonach die Weitergabe der Identität im Rahmen von Ermittlungsverfahren generell möglich, aber auch erforderlich sein müsse. Zuständig für die Abwägungsentscheidung sei allein die jeweils die Herausgabe der Identität anordnende Stelle entsprechend der für sie geltenden gesetzlichen Vorgaben, also etwa im Falle strafrechtlicher Ermittlungen die Staatsanwaltschaft und das Gericht.[241] Auskunftsersuchen staatlicher Stellen müssen immer erforderlich und verhältnismäßig sein, da hier grundsätzlich das Verhältnismäßigkeitsprinzip gilt.[242] In der Praxis kam dagegen bereits vor, dass dieses übersehen wurde.[243] Um potenziell hinweisgebenden Personen die Angst vor einer unbegründeten Ausnahme vom Vertraulichkeitsgrundsatz zu nehmen, sollte § 9 Abs. 2 Nr. 1 HinSchG um die Voraussetzungen der Notwendigkeit und Verhältnismäßigkeit ergänzt werden.[244] Andernfalls könnte der Wortlaut für hinweisgebende Personen abschreckend wirken und sich somit negativ auf die Effektivität des Hinweisgebersystems auswirken. Weiter muss in diesem Zusammenhang ebenfalls bedacht werden, dass die Identität anonymer hinweisgebender Personen für die Weitergabe technisch nachvollzogen werden muss.

[239] Vgl. Dilling, 2022, S. 147.
[240] Vgl. BT-Drs. 20/5992; S. 60f; Bundesregierung, 2023, FH zum HinSchG, S. 71f; Bundesregierung, 2022, RegE zum HinSchG, S. 86.
[241] Vgl. BT-Drs. 20/5992; S. 60f; Bundesregierung, 2023, FH zum HinSchG, S. 71f; Bundesregierung, 2022, RegE zum HinSchG, S. 86.
[242] Vgl. Dilling, 2022, S. 147.
[243] Vgl. EGMR (V. Sektion), 27.4.2017 – 73607/13 (Ulrich Sommer/Deutschland), NJOZ 2019, 455.
[244] Vgl. Dilling, 2022, S. 147.

Gem. § 9 Abs. 3 Nr. 1 HinSchG dürfen Informationen über die Identität der hinweisgebenden Person oder über sonstige Umstände, die Rückschlüsse auf die Identität dieser Person erlauben, weitergegeben werden, wenn die Weitergabe für *Folgemaßnahmen* erforderlich ist. Nach § 9 Abs. 3 Nr. 2 HinSchG muss die hinweisgebende Person zuvor in die Weitergabe eingewilligt haben. Dass, wie in der Entwurfsentscheidung begründet[245], mit § 9 Abs. 3 HinSchG Art. 16 Abs. 1 WBRL umgesetzt wird, ist nicht korrekt.[246] Gründe hierfür sind, dass es für die Vorgabe der Erforderlichkeit von Folgemaßnahmen keine Grundlage in der WBRL gibt und dass angesichts des weiten Wortlautes unklar ist, an wen die Informationen weitergegeben werden dürfen. In Art. 16 WBRL wird geregelt, dass die Identität hinweisgebender Personen nur gegenüber den Mitarbeitern, die zur Entgegennahme der Meldungen oder das Ergreifen von Folgemaßnahmen befugt sind, offengelegt werden darf. So fehlt in § 9 Abs. 3 HinSchG die Nennung dieses begrenzten Personenkreises ebenso wie eine Information wann die Weitergabe für Folgemaßnahmen erforderlich sein soll.[247] Auch hier könnte der unkonkrete Wortlaut ein Grund für eine Nichtmeldung hinweisgebender Personen sein und somit die Effektivität eines Hinweisgebersystems negativ beeinflussen.
In § 9 Abs. 4 HinSchG wird geregelt, dass Informationen über die Identität von Personen, die Gegenstand einer Meldung sind, und von sonstigen in der Meldung genannten Personen an die jeweils zuständige Stelle weitergegeben werden dürfen. Hierfür fehlt es an einer Grundlage in der WBRL, während die Norm zeitgleich zu weitreichend und zu unbestimmt ist.[248] Der wesentliche Schutz der WBRL wird durch die Wahrung der Vertraulichkeit der Identität des Hinweisgebers vermittelt.[249] Art. 22 WBRL nennt zwar Maßnahmen zum Schutz betroffener Personen, beschränkt sich aber in Abs. 2 und Abs. 3 auf Schutz im Rahmen externer Meldungen.[250] Es fehlt hier an speziellen Vorschriften zu Maßnahmen zum Schutz bei internen Meldungen. Gem. der Entwurfsentscheidung gilt für den Schutz der Identität von Personen, die Gegenstand einer Meldung sind, im Grundsatz gem. § 8 HinSchG das gleiche Schutzniveau wie für die Identität der hinweisgebenden Personen. Es sollen

[245] Vgl. BT-Drs. 20/5992; S. 61; Bundesregierung, 2023, FH zum HinSchG, S. 72; Bundesregierung, 2022, RegE zum HinSchG, S. 87.
[246] Vgl. Dilling, 2022, S. 147.
[247] Vgl. Dilling, 2022, S. 147.
[248] Vgl. Dilling, 2022, S. 147.
[249] Vgl. Engels, 2020, S. 21; Dilling, 2019, S. 217.
[250] Vgl. Dilling, 2021, S. 66.

Ausnahmen auf solche Fälle beschränkt sein, „in denen der Verstoß nicht anders abgestellt werden kann“[251], was aber nicht im Wortlaut der Norm zu finden ist. An dieser Stelle können auch datenschutzrechtliche Schadenersatzansprüche gem. Art. 82 Abs. 2 DSGVO, Geldbußen gem. Art. 83 Abs. 2 DSGVO i.V.m. § 43 BDSG und Freiheits- oder Geldstrafen gem. § 42 Art. 2 und 3 BDSG auf Unternehmen zukommen. Der Grund hierfür ist die Verarbeitung und Weitergabe von personenbezogenen Daten ohne Einwilligung der hinweisgebenden Person gem. Art. 6 lit. f DSGVO i.V.m. § 26 Abs. 1 S. 2 BDSG und Art. 6 lit. c DSGVO i.V.m. § 26 Abs. 1 S. 2 BDSG, wenn die Daten ohne rechtliche Grundlage herausgegeben werde und somit das Vertraulichkeitsgebot inkorrekter Weise umgangen wird. Ebenso könnte ein Konflikt mit den datenschutzrechtlichen Informationspflichten und Auskunftsrechte betroffener Personen gem. Art. 14 und 15 DSGVO entstehen.

IX. Interne Untersuchungen als Folgemaßnahme

Gem. § 17 Abs. 1 Nr. 6 HinSchG müssen interne Meldestellen Folgemaßnahmen nach § 18 ergreifen. Folgemaßnahmen sind gem. § 3 Abs. 7 HinSchG von einer Meldestelle ergriffene Maßnahmen zur Prüfung der Stichhaltigkeit einer Meldung, zum weiteren Vorgehen gegen den gemeldeten Verstoß oder zum Abschluss des Verfahrens. Zu den Folgemaßnahmen gehört u. a. gem. § 18 Nr. 1 HinSchG die *Durchführung interner Untersuchungen* beim Beschäftigungsgeber oder bei der jeweiligen Organisationseinheit und die Kontaktierung betroffener Personen und Arbeitseinheiten.

Weitere Informationen zu internen Ermittlungen lassen sich im HinSchG nicht finden. Gem. der Entwurfsbegründung kann die konkrete Ausgestaltung im Rahmen der gesetzlichen Vorgaben individuell entsprechend der Größe und sonstiger Faktoren erfolgen.[252] An gerade diesen Regelungen fehlt es aber, da das VerSanG nicht verabschiedet wurde.[253] Art. 22 Abs. 1 WBRL sieht ausdrücklich *Verfahrensrechte* der von einer Meldung betroffenen Personen vor. Umso bedenklicher ist es, dass im HinSchG keine Informationen zu den Verfahrensrechten im Zusammenhang mit internen Ermittlungen zu finden sind.[254] Gem. Art. 17 Abs. 2 S. 3 HinSchG sollen die Rechte

[251] Vgl. BT-Drs. 20/5992; S. 61; Bundesregierung, 2023, FH zum HinSchG, S. 72; Bundesregierung, 2022, RegE zum HinSchG, S. 87.
[252] Vgl. BT-Drs. 20/5992; S. 68; Bundesregierung, 2023, FH zum HinSchG, S. 81; Bundesregierung, 2022, RegE zum HinSchG, S. 95.
[253] Vgl. Deutsches Institut für Compliance, 2022, S. 2; Dilling, 2022, S. 149.
[254] Vgl. Dilling, 2022, S. 149; European Center for Whistleblower Rights, 2022, S. 1f; Nießen, 2022, S. 400; Transparency International, 2022; S. 10.

der Personen, die Gegenstand einer Meldung sind oder die in der Meldung genannt werden, nicht beeinträchtig werden. Auch die Entwurfsbegründung spricht an zwei Stellen von Verteidigungsrechten betroffener Personen und Personen, die Gegenstand einer Meldung sind.[255] Wie diese Verteidigungsrechte jeweils aussehen, wurde nicht definiert. Um für die nötige Rechtssicherheit zu sorgen, hätte man bspw. die in § 17 Abs. 1 Nr. 5 VerSanG[256] vorgesehenen Verfahrensregeln adaptieren können.[257] Durch die fehlende Erläuterung kann es zu Misstrauen potenzieller hinweisgebender Personen kommen, was sich negativ auf die Effektivität des Whistlelbowingsystems auswirken könnte. Auch muss hier beachtet werden, dass ggf. der Betriebsrat ein Mitbestimmungsrecht haben könnte.[258]

Die *Rückmeldepflicht* nach § 17 Abs. 2 HinSchG ist an dieser Stelle ebenfalls anzusprechen.[259] So muss die interne Meldestelle der hinweisgebenden Person innerhalb von drei Monaten nach der Bestätigung der Meldung eine Rückmeldung geben. Die Rückmeldung muss die Mitteilung geplanter sowie bereits ergriffener Folgemaßnahmen sowie die Gründe für diese umfassen. Der Zweck liegt darin, die hinweisgebende Person in die Lage zu versetzen sich ein Bild davon zu machen, ob ggf. eine anderweitige Folgemeldung oder eine Offenlegung sinnvoll erscheinen und soll somit das Vertrauen in die Wirksamkeit des Hinweisgeberschutzes stärken und insbesondere das Funktionieren des internen Meldekanals verbessern.[260] Ausreichend und sinnvoll wäre hier eine allgemein gehaltene Rückmeldung über die Aktivitäten der Meldestelle, insbesondere ohne Darstellung konkreter Ermittlungsschritte und deren Begründung.[261] Grund hierfür ist, dass die überwiegenden Mehrzahl der Meldungen zu einer Behinderung der internen Untersuchungstätigkeiten oder zur Rechtsgefährdung anderer betroffener Personen führen könnte und somit die als Ausnahme konzipierte Regelung des § 17 Abs. 2 HinSchG oft zur Anwendung käme.[262]

[255] Vgl. BT-Drs. 20/5992; S. 52, 60f; Bundesregierung, 2023, FH zum HinSchG, S. 61, 71f; Bundesregierung, 2022, RegE zum HinSchG, S. 76f, 86.
[256] Vgl. Bundesregierung, 2020, RegE zum VerSanG, S. 14.
[257] Vgl. Deutsches Institut für Compliance, 2022, S. 2; Dilling, 2022, S. 149.
[258] Vgl. Bundesrechtsanwaltskammer, 2022, S.10.
[259] Vgl. Bundesverband der Deutschen Industrie, 2022, S. 12; Deutsches Institut für Compliance, 2022, S. 5.
[260] Vgl. BT-Drs. 20/5992; S. 68; Bundesregierung, 2023, FH zum HinSchG, S. 81; Bundesregierung, 2022, RegE zum HinSchG, S. 94.
[261] Vgl. Bundesverband für Unternehmensjuristen, 2022, S. 7; Deutsches Institut für Compliance, 2022, S. 5f.
[262] Vgl. Deutsches Institut für Compliance, 2022, S. 5f.

Der beschuldigten Person soll idealerweise meist erst in einem späteren Stadium die Eröffnung einer internen Untersuchung über ihr Verhalten preisgegeben werden, damit die Gefahr einer ungerechtfertigten Beschuldigung minimiert und die Beweiserhebung nicht erschwert wird.[263] Dem entgegen steht die *Einschränkung datenschutzrechtlicher Informationspflichten und Auskunftsrechte* betroffener Personen gem. Art. 14 und 15 DSGVO. Gem. Art. 14 DSGVO muss die betroffene Person gem. Abs. 3 lit. a innerhalb eines Monats von der Erlangung der personenbezogenen Daten darüber informieren. Hier könnte die Ausnahmevorschrift des Art. 14 Abs. 5 lit. b DSGVO zum Tragen kommen. So kann die Unterrichtung der betroffenen Person so lange hinausgezögert werden, wie das erhebliche Risiko besteht, dass infolge einer fristgerechten Unterrichtung die Untersuchung der gemeldeten Vorwürfe oder die Erhebung der erforderlichen Beweise gefährdet wird. [264] Fraglich ist, welche Daten dem Betroffenen mitgeteilt werden müssen, wenn dieser Auskunft über seine verarbeiteten Daten einfordert, da gem. Art. 15 Abs. 1 lit. g DSGVO ein Recht auf die Information der Herkunft der Daten besteht. Bei der Einschränkung datenschutzrechtlicher Informationspflichten und Auskunftsrechte betroffener Personen besteht für Unternehmen das Risiko, dass datenschutzrechtliche Schadenersatzansprüche gem. Art. 82 Abs. 2 DSGVO, Geldbußen gem. Art. 83 Abs. 2 DSGVO i.V.m. § 43 BDSG und Freiheits- oder Geldstrafen gem. § 42 Art. 2, 3 BDSG geltend gemacht werden könnten.

X. Zwischenergebnis

Zusammenfassend kann festgehalten werden, dass einige Normen des HinSchG bei der Umsetzung in Unternehmen zu hinterfragen oder zu konkretisieren sind. Verschiedene Schwierigkeiten ergeben sich aus den Bereichen persönlicher und sachlicher Anwendungsbereich, Anreize zur Wahl der internen Meldestelle, zentrale Konzernmeldestelle, anonyme Meldungen, Schutzvoraussetzungen, Repressalienverbot und Beweislastumkehr, Ausnahmen vom Vertraulichkeitsgebot sowie interne Untersuchungen als Folgemaßnahmen. Folgend wird geprüft, ob im Umgang mit diesen rechtlichen Unsicherheiten eine Risiko-BSC ein geeignetes Hilfsmittel ist.

[263] Vgl. Altenbach/Dierkens, 2020, S. 128.
[264] Vgl. Datenschutzkonferenz, 2020, S. 10.

C. Balanced Score Card im Umgang mit dem HinSchG

Wie bereits erläutert, entstehen aus dem neuen HinSchG für Unternehmen bei dessen Umsetzung verschiedene Risiken. Im Folgenden wird untersucht, ob die Anwendung einer Risiko-BSC als Hilfestellung im Umgang mit diesen Risiken dienen kann. Dafür wird zunächst der gewählte Ansatz beschrieben, danach die Risikoidentifizierung, -analyse sowie -bewertung vorgenommen. Abschließend werden die Vorgehensweise und die Anwendungsmöglichkeit der Risiko-BSC bewertet.

I. Gewählter Ansatz

Als mögliches Hilfsmittel für Unternehmen im Umgang mit den Risiken, welche aus der Umsetzung des HinSchG entstehen könnten, wird eine *separate Risiko-BSC,* siehe Abbildung 9, gewählt. Der Grund hierfür ist die isolierte Betrachtung dieser Risiken im Rahmen des CMS unabhängig von der übergeordneten BSC des Unternehmens.

Trotz der isolierten Betrachtung der Risiken, welche sich aus dem HinSchG ergeben, werden die *Perspektiven* der klassischen BSC beibehalten. Der Grund hierfür ist die dadurch mögliche ganzheitliche Sichtweise auf das Unternehmen. Auch Compliance, deren Prozesse und Instrumente stehen in Zusammenhang mit nahezu allen Unternehmensbereichen. Die genannten Risiken können unternehmensweit auftreten, sodass eine Gesamtschau an dieser Stelle sinnvoll ist. Betrachtet werden dabei also die finanzielle Perspektive, die Kundenperspektive, die interne (Prozess-)Perspektive sowie die Innovations- und Lernperspektive, siehe Abbildung 9.

Während die *Leitfragen* der internen (Prozess-)Perspektive und der Innovations- und Lernperspektive die gleichen bleiben wie bei der klassischen BSC, müssen die der finanziellen Perspektive und der Kundenperspektive bei der Betrachtung der Risiken aus der Umsetzung des HinSchG angepasst werden, wie in Abbildung 10 dargestellt. Möglich ist dies, da die klassische BSC und deren Perspektiven kein starres Konzept abbilden, sondern unternehmensspezifisch angepasst und ergänzt werden können.

Die *Inhalte*, die innerhalb der Perspektiven unter Beachtung der Leitfragen zum Tragen kommen, werden im Vergleich zur klassischen BSC ebenfalls leicht abgewandelt. So befasst sich die finanzielle Perspektive nun mit der Einhaltung des Budgets. Die Innovations- und Lernperspektive betrachtet die kontinuierliche Verbesserung operativer Effektivität.

II. Prozess der Risikoableitung

Der *Prozess der Risikoableitung,* siehe Abbildung 11, ähnelt zu Beginn dem der Zielableitung der klassischen BSC, siehe Abbildung 6. Zunächst werden die Risiken mit Hilfe der vier Perspektiven der klassischen BSC systematisch erfasst, indem diese identifiziert, aggregiert und den Perspektiven zugeordnet werden. Anstelle der Definition von Messgrößen folgt aber, wie aus Tabelle 2 ersichtlich, eine Analyse der Risikoursachen, Eintrittswahrscheinlichkeiten und Schadenshöhen der Risiken. Dieses Vorgehen wird gewählt, das der Umgang mit Risiken und nicht der Umgang mit strategischen Zielen im Fokus steht. Das Vorgehen unterhalb der einzelnen Schritte wird anschließend erläutert.

1. Risikoerfassung

Zunächst werden die möglichen Risiken anknüpfend an die Ausführungen aus Kapitel B erfasst, inhaltlich konkretisiert und ergänzt. Dies erfolgt je Themengebiet aus Kapitel B, da auch schon die Analyse der rechtlichen Unsicherheiten in diesen Kategorien erfolgte und sich diese um mögliche aus ihnen resultierende Risiken erweitern lässt.

Im Zusammenhang mit dem *persönlichen Anwendungsbereich* könnte es zu negativen Auswirkungen auf die Effektivität es Hinweisgebersystems eines Unternehmens kommen. Gründe hierfür sind, dass relevante Informationen über mögliche Verstöße verloren gehen, das Vertrauen in das Hinweisgebersystem schwindet oder potenzielle hinweisgebende Personen von einer Meldung zurückschrecken. Ebenso fließen hier mögliche Verzögerungen der Hinweisbearbeitung durch aufwändige Prüfung des Anwendungsbereiches ein. Das könnte wiederum zu Verletzungen der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB führen. Weiter sind ein organisatorischer Mehraufwand, Kosten für steigenden Personalaufwand und die Einrichtung technischer Lösungen denkbar. Sollten technische Einrichtungen verwendet werden, muss der Betriebsrat gem. § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG einbezogen werden, da sonst ein Risiko der Zahlung von Ordnungs- oder Zwangsgeld gem. Art. 23 Abs. 3 S. 1, 2 BetrVG besteht. Ebenso könnte das Risiko einer Bußgeldzahlung gem. § 40 Abs. 2 Nr. 1 HinSchG bestehen, da eine Behinderung einer Meldung bestehen könnte. Weiter droht das Risiko eines negativen Einflusses auf die Unternehmenskultur durch Unsicherheiten und

mangelndes Vertrauen in das CMS, worauf womöglich auch Reputationsschäden folgen könnten.

Aus den Unsicherheiten bezogen auf den s*achlichen Anwendungsbereich* des HinSchG könnten hinweisgebende Personen ebenfalls vor einer Meldung zurückschrecken. Dieser Umstand könnte sich negativ auf die Effektivität des Whistleblowersystems eines Unternehmens auswirken. Auch dies könnte Verletzungen der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB begünstigen. Weiter könnten deliktische Haftungsansprüche oder die Verletzung von Sorgfaltspflichten zu Nachteilen für Unternehmen führen. Auch muss mit finanziellen Mehrkosten für Personal und organisatorischem Mehraufwand gerechnet werden. Ebenso sind zusätzliche Kosten für die Einrichtung technischer Lösungen möglich. Hierbei zu beachten ist, dass der Betriebsrat gem. § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG einbezogen werden muss, da sonst ein Risiko der Zahlung von Ordnungs- oder Zwangsgeld gem. Art. 23 Abs. 3 S. 1, 2 BetrVG besteht. Auch könnte eine Bußgeldzahlung gem. § 40 Abs. 2 Nr. 1 HinSchG aufgrund der Behinderung einer Meldung auf das Unternehmen zukommen. Durch Unsicherheiten könnte mangelndes Vertrauen in Compliance entstehen und die Unternehmenskultur negativ beeinflussen, was zu Reputationsschäden führen könnte.

Fehlende *Anreize zur Wahl der internen Meldestelle* könnten für Unternehmen aufgrund nicht rechtzeitiger Durchführung von Gegenmaßnahmen zur Abwendung von Straftaten und somit zu Geldbußen oder Imageschäden führen. Durch Ausbleiben interner Hinweise könnte es zu einer Ineffektivität des Hinweisgebersystems kommen und somit zu Verletzungen der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB. Ebenfalls könnte eine Bußgeldzahlung gem. § 40 Abs. 2 Nr. 2 HinSchG fällig werden, da eine interne Meldestelle nicht eingerichtet ist oder nicht korrekt betrieben wird. Auch kommen auf das Unternehmen möglicherweise ein organisatorischer Mehraufwand und erhöhte Personalkosten zu. Ebenfalls könnte es zu Unsicherheit in der Belegschaft kommen, was sich negativ auf die Unternehmenskultur auswirken kann.

Sowohl die Einrichtung als auch die Nichteinrichtung einer *zentralen Konzernmeldestelle* könnten sich je nach vorhandenen Gegebenheiten

negativ auf die Effektivität des internen Meldekanals auswirken und zu Mehrkosten und Verzögerungen bei der Hinweisbearbeitung oder Umgehung interner Prozesse führen. Eine solche Ineffektivität könnte Verletzungen der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB begünstigen. Weiter ist fraglich, ob sich für deutsche Unternehmen durch die unterschiedliche Auffassung des deutschen Gesetzgebers und der Europäischen Kommission Nachteile ergeben könnten. Ebenso könnten datenschutzrechtliche Schadenersatzansprüche gem. Art. 82 Abs. 2 DSGVO, Geldbußen gem. Art. 83 Abs. 2 DSGVO i.V.m. § 43 BDSG und Freiheits- oder Geldstrafen gem. § 42 Art. 2, 3 BDSG auf Unternehmen zukommen. Das Risiko der Zahlung von Ordnungs- oder Zwangsgeld gem. Art. 23 Abs. 3 S. 1, 2 BetrVG kann bestehen, da womöglich nicht der korrekte Betriebsrat (lokaler Betriebsrat oder Konzernbetriebsrat) einbezogen wird. Individualrechtliche Konsequenzen könnten aus einem Verstoß der Sorgfaltspflicht des Arbeitgebers folgen, da die Bearbeitung des Hinweises und mögliche Folgemaßnahmen nicht in der richtigen Entität erfolgen. In diesem Zusammenhang kann es auch zu Prozesskosten, Gehaltsnachzahlungen oder Abfindungszahlungen aufgrund ungerechtfertigter Kündigung kommen. Bußgeldzahlung gem. § 40 Abs. 6 i.V.m. Abs. 2 Nr. 3 und Abs. 3 HinSchG könnten ebenfalls folgen. Grund hierfür könnten das Ergreifen von Repressalien oder ein Verstoß gegen das Vertraulichkeitsgebot sein. Auch die Unternehmenskultur könnte negativ beeinflusst werden, da es zu Unsicherheiten und schwindendem Vertrauen in das CMS kommen kann.

Durch die fehlende Möglichkeit zur *anonymen Hinweisgabe* würde die Hemmschwelle einiger potenzieller hinweisgebender Personen nicht abgebaut werden. Zum einen gehen dadurch wesentliche Erkenntnisquellen verloren, zum anderen könnte das Hinweisgebersystem jedoch aufgrund von Meldemissbrauch und unberechtigter Denunziation überlastet werden. Beides könnte sich negativ auf die Effektivität der internen Meldestelle auswirken. Somit könnte es zu Verletzungen der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB kommen. Ein weiteres Risiko sind steigende Kosten für Personal und Technik. Beim Einsatz technischer Mittel müsste der Betriebsrat eingebunden werden, wodurch ein Risiko der Zahlung von

Ordnungs- oder Zwangsgeld gem. Art. 23 Abs. 3 S. 1, 2 BetrVG auf das Unternehmen zukommen könnte. Auch besteht ein Risiko bezüglich datenschutzrechtlicher Schadenersatzansprüche gem. Art. 82 Abs. 2 DSGVO, Geldbußen gem. Art. 83 Abs. 2 DSGVO i.V.m. § 43 BDSG oder Freiheits- oder Geldstrafen gem. § 42 Art. 2, 3 BDSG. Geldbußen könnten aufgrund § 40 Abs. 6 i.V.m. Abs. 2 Nr. 1 und Abs. 3 HinSch auf das Unternehmen zukommen, da Meldungen behindert werden könnten oder gegen das Vertraulichkeitsgebot verstoßen werden könnte. Die Unternehmenskultur könnte durch Denuziantentum und Unsicherheiten leiden, was auch zu Imageschäden führen könnte.

Eine der *Voraussetzungen für den Schutz* hinweisgebender Personen ist die Gutgläubigkeit. Hier kann es aufgrund von Unsicherheiten zur Abschreckung potenzieller Hinweisgeber kommen, was sich auf die Unternehmenskultur, das Image und wiederum auf die Effektivität des Hinweisgersystems auswirken kann. Daraus könnten Verletzungen der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB folgen. Möglicherweise könnte ein Verstoß gegen die Sorgfaltspflicht des Arbeitgebers Folgen nach sich ziehen. Im Zusammenhang mit *Repressalienverbot und Beweislastumkehr* könnten Geldstrafen gem. § 40 Abs. 2 Nr. 3 HinSchG auf Unternehmen zukommen. Weiter ist ein Imageschaden möglich. Auch könnten potenzielle hinweisgebende Personen vor einer Meldung oder Offenlegung eines Verstoßes abgeschreckt werden und damit die Effektivität des Hinweisgebersystems negativ beeinflusst werden. Dies könnte zu Verletzungen der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB führen. Die Möglichkeit vermehrter Kündigungsschutzklagen könnten für Arbeitgeber zu finanziellem Mehraufwand in Form von Prozesskosten, Gehaltsnachzahlungen und Abfindungzahlungen führen. Auch kollektivarbeitsrechtliche Konsequenzen könnten aus dem besonderen Kündigungsschutz gem. § 15 Abs. 4 KSchG von Betriebsratsmitgliedern folgen, da sie unter den Begriff Mittler fallen könnten. Hier könnte es auch zu Kündigungsschutzklagen aufgrund unbegründeter Kündigung kommen. Auch kann es zu datenschutzrechtlichen Schadenersatzansprüchen gem. Art. 82 Abs. 2 DSGVO, Geldbußen gem. Art. 83 Abs. 2 DSGVO i.V.m.

§ 43 BDSG und Freiheits- oder Geldstrafen gem. § 42 Art. 2, 3 BDSG kommen. Weiter können deliktische Haftungsansprüche oder die Verletzung von Sorgfaltspflichten zu Nachteilen für Unternehmen führen. Ebenso besteht die Möglichkeit, dass aufgrund von Angst und Unsicherheiten das Vertrauen in das CMS schwindet und ein Reputationsschaden folgt.

Bezüglich des *Vertraulichkeitsgebots und dessen Ausnahmen* kann es zu einem ineffizienten internen Meldekanal kommen und somit zu Verletzungen der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB. Ebenfalls können auf Unternehmen sowohl Sanktionszahlungen gem. § 40 Abs. 6 i.V.m. Abs. 2 Nr. 3 HinSchG als auch datenschutzrechtliche Schadenersatzansprüche gem. Art. 82 Abs. 2 DSGVO, Geldbußen gem. Art. 83 Abs. 2 DSGVO i.V.m. § 43 BDSG oder Freiheits- oder Geldstrafen gem. § 42 Art. 2, 3 BDSG zukommen. Auch könnte es hier zu Bußgeldzahlungen gem. § 40 Abs. 6 i.V.m. Abs. 2 Nr. 3 HinSchG kommen, da gegen das Repressalienverbot verstoßen werden könnte. Neben organisatorischem Mehraufwand und zusätzlicher Personalkosten könnte der Arbeitgeber gegen seine Sorgfaltspflicht verstoßen oder aufgrund ungerechtfertigter Kündigungen Prozesskosten, Gehaltszahlungen oder Abfindungszahlungen tragen müssen. Mitarbeitende könnten aufgrund Unsicherheit Vertrauensprobleme in die Wirksamkeit des Hinweisgeberschutzes im Rahmen des CMS bekommen, was in der Außenwirkung zu Imageschäden führen könnte.

Interne Untersuchungen als Folgemaßnahme können sich negativ auf die Effektivität des Whistleblowersystems auswirken, da potenzielle hinweisgebende Personen misstrauisch werden könnten und somit eine Meldung ausbleiben kann. So könnten Verletzungen der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB entstehen. Weiter könnte es hier zum Risiko der Zahlung von Ordnungs- oder Zwangsgeld gem. Art. 23 Abs. 3 S. 1, 2 BetrVG kommen. Auch möglich können datenschutzrechtliche Schadenersatzansprüche gem. Art. 82 Abs. 2 DSGVO, Geldbußen gem. Art. 83 Abs. 2 DSGVO i.V.m. § 43 BDSG und Freiheits- oder Geldstrafen gem. § 42 Art. 2, 3 BDSG sein. Zu Bußgeldern gem. § 40 Abs. 6 i.V.m. Abs. 2 Nr. 3 und Abs. 3 HinSchG könnte es auch kommen, da gegen das Repressalienverbot und das Vertraulichkeitsgebot verstoßen werden könnte.

Auch ist sind eine Zahlung von Ordnungs- oder Zwangsgeld gem. Art. 23 Abs. 3 S. 1 und 2 BetrVG, da sich aus § 80 Abs. 2 S. 1 BetrVG entsprechende Auskunftsrechte ergeben könnten. Weiter können deliktische Haftungsansprüche oder die Verletzung von Sorgfaltspflichten zu Nachteilen für Unternehmen führen. Auch die fehlenden Regelungen bezüglich interner Untersuchungen könnten zu einem Vertrauensverlust in das CMS und zu Reputationsschäden führen.

2. Bildung von Risikoclustern

Unter Zuhilfenahme einer tabellarischen Aufstellung, siehe Tabellen 3 bis 5, können die identifizierten und konkretisierten Risiken in folgende *Kategorien* zusammengefasst werden:

- Zusatzkosten durch technische Einrichtungen und steigenden Personalbedarf
- Sanktionen aus dem HinSchG
- Geldstrafen/OWiG durch Verletzung der Legalitätspflicht
- Datenschutzrechtliche Schadenersatzansprüche, Geldbußen und Freiheitsstrafen
- Kollektivarbeitsrechtliches Ordnungs- oder Zwangsgeld
- Individualarbeitsrechtliche Schadenersatzzahlungen, Prozesskosten, Gehalts- und Abfindungszahlungen
- Ineffektivität des Hinweisgebersystems
- Negative Auswirkungen auf die Unternehmenskultur, Vertrauensverlust in das Hinweisgebersystem/CMS
- Nichteinhaltung interner Prozesse, nicht abgestimmte Handlungen
- Reputationsschäden

Tabelle 3: Identifizierung und Aggregierung der Risiken aus dem HinSchG, Teil 1

	Persönlicher Anwendungsbereich	Sachlicher Anwendungsbereich	Anreize interne Meldestelle
Zusatzkosten	Zusätzlicher Personalaufwand zur Prüfung, ob persönlicher Anwendungsbereich eröffnet ist	Zusätzlicher Personalaufwand zur Prüfung, ob sachlicher Anwendungsbereich eröffnet ist	Zusätzliche Personalkosten
	Zusatzkosten durch technische Einrichtung zur Prüfung, ob persönlicher Anwendungsbereich eröffnet ist	Zusatzkosten durch technische Einrichtung zur Prüfung, ob sachlicher Anwendungsbereich eröffnet ist	
Sanktionen aus HinSchG	§ 40 Abs. 6 i.V.m. Abs. 2 Nr. 1 HinSchG	§ 40 Abs. 6 i.V.m. Abs. 2 Nr. 1 HinSchG	§ 40 Abs. 6 i.V.m. Abs. 2 Nr. 2 HinSchG
Geldstrafen/OWiG	Verletzung der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB	Verletzung der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB Deliktische Haftungsansprüche wegen fehlender Meldung bei Verstößen gegen interne Vorgaben	Verletzung der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB
Datenschutzrecht			
Schadenersatzanspruch gem. Art. 82 Abs. 2 DSGVO	-	-	-
Geldbuße gem. Art. 83 Abs. 2 DSGVO i.V.m. § 43 BDSG			
Freiheits- oder Geldstrafe gem. § 42 Art 2, 3 BDSG			
Kollektivarbeitsrecht			
Ordnungs- oder Zwangsgeld gem. Art 23 Abs. 3 S. 1, 2 BetrVG	Einbeziehen des Betriebsrats gem. § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG bei Einsatz technischer Lösung	Einbeziehen des Betriebsrats gem. § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG bei Einsatz technischer Lösung	-
Prozesskosten, Gehaltsnachzahlung, Abfindungszahlung	-	-	
Individualarbeitsrecht	-	Verletzung von Sorgfaltspflichten wegen fehlender Meldung bei Verstößen gegen interne Vorgaben	-
Ineffektivität des Hinweisebersystems	Ausbleibende Hinweisgabe aus Angst nicht in den persönlichen Anwendugsbereich zu fallen	Ausbleibende Hinweisgabe aus Angst nicht in den sachlichen Anwendugsbereich zu fallen	Ausbleiben interner Hinweise
	Ausbleibende Hinweisgabe aus Angst vor Repressalien gegen Mittler und Dritte	Zeitliche Verzögerung der Hinweisbearbeitung durch aufwändige Prüfung	
	Zeitliche Verzögerung der Hinweisbearbeitung durch aufwändige Prüfung		
Interne Prozesse	Organisatorischer Mehraufwand	Organisatorischer Mehraufwand	Organisatorischer Mehraufwand
Unternehmenskultur	Unsicherheiten, Mangeldes Vertrauen in CMS	Unsicherheiten, Mangeldes Vertrauen in CMS	Unsicherheiten, Mangeldes Vertrauen in CMS
Reputationsschaden	Nichteffizienz Hinweisgebersystem als Teil des CMS	Nichteffizienz Hinweisgebersystem als Teil des CMS	Nichteffizienz Hinweisgebersystem als Teil des CMS Nicht rechtzeitige Abwendung von Geldbußen/Strafverfahren

Tabelle 4: Identifizierung und Aggregierung der Risiken aus dem HinSchG, Teil 2

Zentrale Konzernmeldestelle	Anonyme Hinweisgabe	Schutzvoraussetzungen
Zusatzkosten	Zusätzlicher Personalaufwand durch Bearbeitung steigender Meldungen und Einsatz von Ombudspersonen	-
	Zusatzkosten durch notwendige technische Einrichtungen, um trotz Wahrung der Anonymität Hinweisgeber über Empfang und Ergebnis zu unterrichten und ggf. Rückfragen stellen zu können	
Sanktionen aus HinSchG	§ 40 Abs. 6 i.V.m. Abs. 2 Nr. 1 HinSchG § 40 Abs. 6 i.V.m. Abs. 3 HinSchG	-
Geldstrafen/OWiG	Verletzung der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB Ggf. rechtliche Probleme wegen Ansicht der EU Kommission	-
Datenschutzrecht		
Schadenersatzanspruch gem. Art. 82 Abs. 2 DSGVO Geldbuße gem. Art. 83 Abs. 2 DSGVO i.V.m. § 43 BDSG Freiheits- oder Geldstrafe gem. § 42 Art 2, 3 BDSG	Verarbeitung und Weitergabe von personenbezogenen Daten ohne Einwilligung außerhalb der Entität, in der der Hinweisgeber arbeitet, Art. 6 lit. f DSGVO i.V.m. § 26 Abs. 1 S. 2 BDSG, Art. 6 lit. c DSGVO i.V.m. § 26 Abs. 1 S. 2 BDSG	Konflikt der Interessen des Hinweisgebers und betroffener Personen, Einschränkung datenschutzrechtlicher Informationspflichten und Auskunftsrechte betroffener Personen gem. Art. 14 und 15 DSGVO
Kollektivarbeitsrecht		
Ordnungs- oder Zwangsgeld gem. Art 23 Abs. 3 S. 1, 2 BetrVG	Welcher Betriebsrat muss einbezogen werden? Gesamtbetriebsrat bzw. Konzernbetriebsrat, der lokale oder beide? Einbeziehen des Betriebsrats gem. § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG bei technischer Lösung	Einbeziehen des Betriebsrats gem. § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG bei technischer Lösung, um mit anonymen Hinweisgeber kommunizieren zu können
Prozesskosten, Gehaltsnachzahlung, Abfindungszahlung	-	-
Individualarbeitsrecht	Verstoß gegen die Sorgfaltspflicht durch Arbeitgeber, da die Sicherstellung ggf. nicht in der richtigen Entität erfolgt	-
	Prozesskosten, Gehaltsnachzahlung, Abfindungszahlung wg. ungerechtfertigter Kündigung	Verstoß gegen die Sorgfaltspflicht durch Arbeitgeber
Ineffektivität des Hinweisebersystems	Ausbleibende Hinweisgabe aus Angst vor Aufdeckung der Identität und Repressalien, fehlendes Vertrauen	Ausbleibende Hinweisgabe aus Angst vor Aufdeckung der Identität und Repressalien, fehlendes Vertrauen
	Zeitliche Verzögerung der Hinweisbearbeitung	Überlastung wegen Meldemissbrauch und unberechtigter Denunziation
	Ungleiches Vorgehen verschiedener Stellen und dadurch Vertrauensverlust der Hinweisgeber	Ausbleibende Hinweisgabe aus Angst vor Aufdeckung der Identität und Repressalien, fehlendes Vertrauen
Interne Prozesse	Umgehen zentraler interner Prozesse	Organisatorischer Mehraufwand
Unternehmenskultur	Unsicherheiten, Mangelndes Vertrauen in CMS	Mangelndes Vertrauen in CMS
Reputationsschaden	Nichteffizienz Hinweisgebersystem als Teil des CMS	Nichteffizienz Hinweisgebersystem als Teil des CMS

Tabelle 5: Identifizierung und Aggregierung der Risiken aus dem HinSchG, Teil 3

	Repressalienverbot/Beweislastumkehr	Vertraulichkeitsgebot und Ausnahmen	Interne Untersuchungen
Zusatzkosten	Zusätzlicher Personalaufwand	Zusätzlicher Personalaufwand	Zusätzlicher Personalaufwand
Sanktionen aus HinSchG	§ 40 Abs. 6 i.V.m. Abs. 3 HinSchG	§ 40 Abs. 6 i.V.m. Abs. 2 Nr. 3 HinSchG	§ 40 Abs. 6 i.V.m. Abs. 2 Nr. 3 HinSchG
Geldstrafen/OWiG	Verletzung der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB	Verletzung der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB	Verletzung der Legalitätspflicht gem. § 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG i.V.m. § 130 OWiG und § 266 Abs. 1 StGB
Datenschutzrecht			
Schadenersatzanspruch gem. Art. 82 Abs. 2 DSGVO Geldbuße gem. Art. 83 Abs. 2 DSGVO i.V.m. § 43 BDSG Freiheits- oder Geldstrafe gem. § 42 Art 2, 3 BDSG	Verletzung der Löschpflicht gem. Art. 17 Abs. 1 lit. a DSGVO	Verarbeitung und Weitergabe von personenbezogenen Daten ohne Einwilligung Art. 6 lit. f DSGVO i.V.m. § 26 Abs. 1 S. 2 BDSG, Art. 6 lit. c DSGVO i.V.m. § 26 Abs. 1 S. 2 BDSG Einschränkung datenschutzrechtlicher Informationspflichten und Auskunftsrechte betroffener Personen gem. Art. 14 und 15 DSGVO	Einschränkung datenschutzrechtlicher Informationspflichten und Auskunftsrechte betroffener Personen gem. Art. 14 und 15 DSGVO
Kollektivarbeitsrecht			
Ordnungs- oder Zwangsgeld gem. Art 23 Abs. 3 S. 1, 2 BetrVG	-	-	Auskunftsansprüche des Betriebsrates aus § 80 Abs. 2 S. 1 BetrVG
Prozesskosten, Gehaltsnachzahlung, Abfindungszahlung	Betriebsrat als Mittler, besonderer Kündigungsschutz, § 15 Abs. 4 KSchG, Kündigungsschutzklage bei unbegründeter Kündigung	-	-
Individualarbeitsrecht	Verstoß gegen die Sorgfaltspflicht durch Arbeitgeber Prozesskosten, Gehaltsnachzahlung, Abfindungszahlung wg. ungerechtfertigter Kündigung	Verstoß gegen die Sorgfaltspflicht durch Arbeitgeber	Verstoß gegen die Sorgfaltspflicht durch Arbeitgeber
Ineffektivität des Hinweisebersystems	Ausbleibende Hinweisgabe aus Angst vor Aufdeckung der Identität und Repressalien, fehlendes Vertrauen Überlastung wegen Meldemissbrauch und unberechtigter Denunziation	Ausbleibende Hinweisgabe aus Angst vor Aufdeckung der Identität und Repressalien, fehlendes Vertrauen	Ausbleibende Hinweisgabe aus Angst vor Aufdeckung der Identität und Repressalien, fehlendes Vertrauen
Interne Prozesse	Organisatorischer Mehraufwand	Organisatorischer Mehraufwand	Organisatorischer Mehraufwand
Unternehmenskultur	Mangeldes Vertrauen in CMS	Mangeldes Vertrauen in CMS	Mangeldes Vertrauen in CMS
Reputationsschaden	Nichteffizienz Hinweisgebersystem als Teil des CMS	Nichteffizienz Hinweisgebersystem als Teil des CMS	Nichteffizienz Hinweisgebersystem als Teil des CMS

Um nun aber dem Aufbau der vier Perspektiven der Risiko-BSC gerecht zu werden, werden die identifizierten und geclusterten Risiken diesen zugeordnet, siehe Abbildung 12.

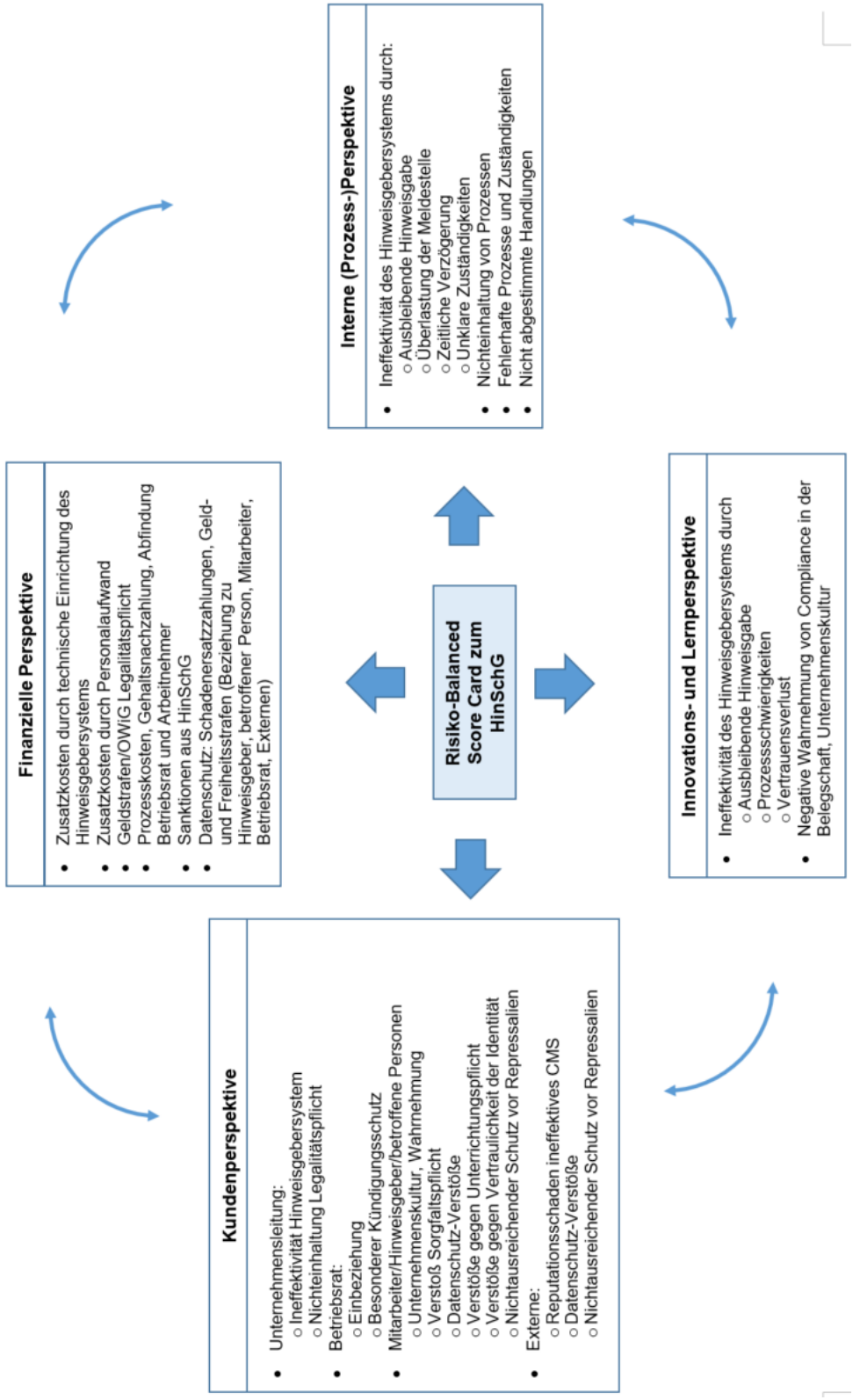


Abbildung 12: Risiko-BSC zum HinSchG

Dabei müssen die Leitfragen und Inhalte aus Abbildung 10 beachtet werden:

- Finanzielle Perspektive: Welche finanziellen Vorgaben müssen wir erfüllen? - Einhaltung des Budgets
- Kundenperspektive: Wie nehmen uns (als Compliance) Unternehmensleitung, Betriebsrat, Mitarbeiter und Externe wahr? - Ziele für Zeit, Qualität, Performance und Service
- Interne (Prozess-)Perspektive: Wo müssen wir besonders gut sein? - Prozesse, Entscheidungen und Handlungen
- Innovations- und Lernperspektive: Wo können wir uns verbessern und Wert schaffen? - Kontinuierliche Verbesserung operativer Effizienz

Abbildung 12 zeigt durch Zuordnung der in Kapitel C. II. 1 identifizierten Risiken zu den vier Perspektiven die *Risiko-BSC zum HinSchG*.

Die *finanzielle Perspektive* umfasst Zusatzkosten durch technische Einrichtung der Meldekanäle und zusätzlichen Personalmehraufwand sowie Geldstrafen/OWiG durch Verletzung der Legalitätspflicht. Ebenso lassen sich hier mögliche Prozesskosten, Gehaltszahlungen und Abfindungszahlungen an Arbeitnehmer und Betriebsratsmitglieder finden. Auch Sanktionszahlungen aus dem HinSchG lassen sich hier zuordnen sowie datenschutzrechtliche Folgen in Form von Geldstrafen.

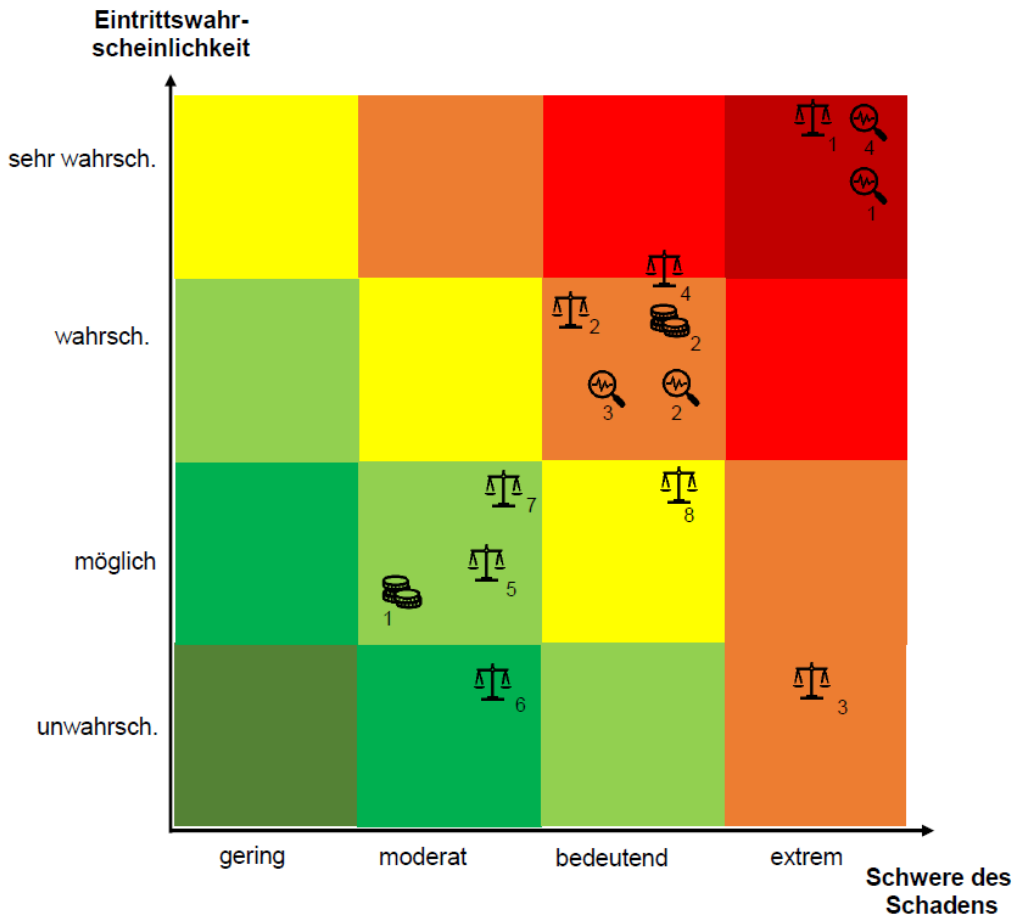
Die *Kundenperspektive* wird aufgeteilt in die Unterabschnitte Unternehmensleitung, Betriebsrat, Mitarbeiter/hinweisgebende Personen/betroffene Personen und Externe. Der Unternehmensleitung zugeordnet werden die Ineffektivität des Hinweisgebersystems sowie die Verletzung der Legalitätspflicht. Der Betriebsrat muss in Entscheidungen einbgezogen werden und genießt einen besonderen Küdigungsschutz. In der Beziehung zu Mitarbeitern, hinweisgebenden und betroffenen Personen können Risiken hinsichtlich Unternehmenskultur, Verstöße gegen die Sorgfaltspflicht und datenschutzrechtliche Verstöße sowie Verstöße gegen die Unterrichtungspflicht, das Vertraulichkeitsgebot und das Repressalienverbot aus dem HinSchG entstehen. Externe könnten ein ineffektives CMS, Datenschutzverstöße oder den nicht ausreichendem Schutz vor Repressalien wahrnehmen, was zu Reputationsschäden führen könnte.

Der *internen (Prozess-)Perspektive* werden die Ineffektivität des Hinweisgebersystems hinsichtlich ausbleibender Meldungen, die Überlastung der Meldestelle, die Verzögerung und unklarer Zuständigkeiten sowie die Nichteinhaltung von Prozessen, fehlerhafte Prozesse und Zuständigkeiten sowie nicht abgestimmte Handlungen zugeordnet.

Die *Innovations- und Lernperspektive* umfasst die Ineffektivität des Hinweisgebersystems hinsichtlich ausbleibender Meldungen, Prozessschwierigkeiten und Vertrauensverlust. Auch die negative Wahrnehmung von Compliance in der Belegschaft und die damit verbundenen negativen Auswirkungen auf die Unternehmenskultur lassen sich hier finden.

3. Risikobewertung

An dieser Stelle sollte im Rahmen der *Risikobewertung* die Risiko-BSC um Eintrittswahrscheinlichkeiten und Schadenshöhe der einzelnen Risiken erweitert werden, siehe Abbildung 11. Wie bereits erläutert eignen sich Risiken aus dem Compliance-Bereich wenig für eine quantitative Risikobewertung. Für eine qualitative Risikobewertung wurde eine separate Risikomatrix als Hilfestellung erstellt, siehe Abbildung 13.



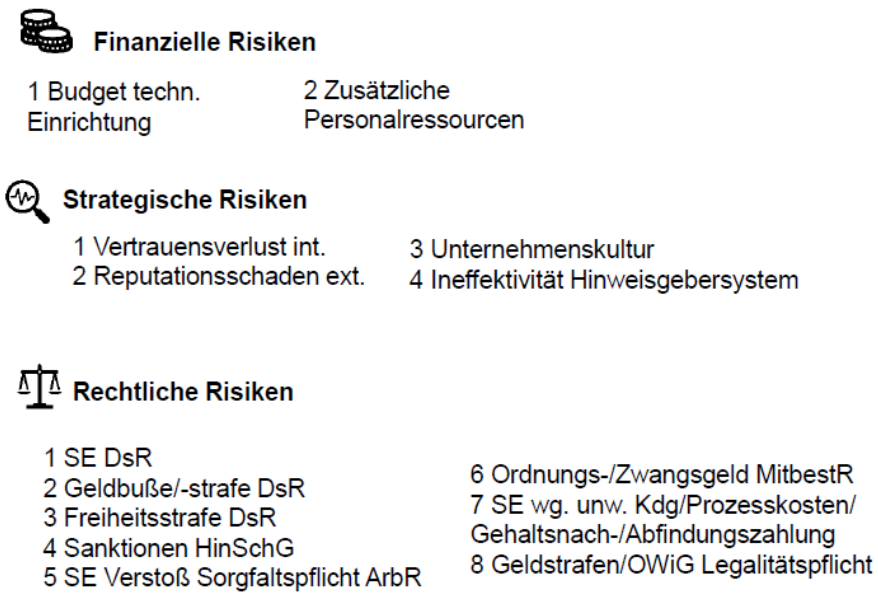


Abbildung 13: Risikomatrix zum HinSchG

Mithilfe einer *Risikomatrix* werden die verschiedenen Risiken auf der x-Achse nach Schwere des Schadens und auf der y-Achse nach Eintrittswahrscheinlichkeit zugeordnet. Die Schwere des Schadens wurde kategorisiert in gering, modreat, bedeutend und extrem. Die Eintrittswahrscheinlichkeit wurde wie folgt kategorisiert: sehr wahrscheinlich, wahrscheinlich, möglich, unwahrscheinlich. Je höher die Schwere des Schadens und die Eintrittswahrscheinlichkeit für das Unternehmen sind, desto weiter rechts und oben wurde das Risiko in der Risikomatrix angeordnet. Farbliche Abstufungen tragen zur besseren Visualisierung bei.

Aus der Risikomatrix zum HinSchG lassen sich folgende *Aussagen* ableiten:

- Als moderat und unwahrscheinlich lässt sich die Zahlung von Ordnungs- und Zwangsgeld aus dem BetrVG einstufen.
- Die Risiken der Überschreitung des finanziellen Budgets zur technischen Einrichtung der internen Meldekanäle, Schadenersatzzahlungen aufgrund Verletzung der individualrechtlichen Sorgfaltspflicht und Schadenersatzzahlungen wegen unwirksamer Kündigungen und damit einhergehende Prozesskosten, Gehaltsnach- und Abfindungszahlungen lassen sich als moderat und möglich einstufen.

- Bedeutend und möglich sind Geldstrafen/OWiG wegen Verletzung der Legalitätspflicht.
- Extrem und möglich sind Freiheitsstrafen aufgrund datenschutzrechtlicher Verstöße.
- Finanzieller Mehraufwand bezüglich zusätzlicher Personalkosten, Reputationsschaden, negativer Einfluss auf die Unternehmenskultur sowie Geldbußen/-strafen aufgrund datenschutzrechtlicher Verstöße sind bedeutend und wahrscheinlich.
- Zahlungen von Bußgeld gem. HinSchG sind als bedeutend und zwischen wahrscheinlich und sehr wahrscheinlich einzustufen.
- Extreme und sehr wahrscheinliche Risiken sind die Ineffektivität des Hinweisgebersystems, Vertrauensverlust und Schadenersatzzahlungen aufgrund datenschutzrechtlicher Verstöße.

Die Risiko-BSC wurde also nur zur Risikoidentifikation und -analyse verwendet, nicht zur Risikobewertung. Sie diente aber als Grundlage einer separaten Risikobewertung unter Zuhilfenahme einer Risikomatrix.
Die Ergebnisse aus Risiko-BSC und Risikomatrix zum HinSchG könnten im Anschluss als Basis für die Risikosteuerung, -überwachung und -kommunikation dienen.

III. Bewertung des Vorgehens

Anschließend wird bewertet, ob die Verwendung einer *separaten Risiko-BSC* aus Sicht der Compliance-Abteilung ein geeignetes und sinnvolles Hilfsmittel im Umgang mit den Risiken aus der Umsetzung des HinSchG darstellt. Die hierbei verwendeten Perspektiven, Leitfragen und Inhalte wurden bereits in Kapitel C. I. erläutert.
Man hätte bei der Wahl der Form der BSC auch an die Nutzung einer Compliance-Scorecard[265] denken können. Dadurch, dass in dieser Arbeit aber nur die Compliance-Risiken und nicht das gesamte CMS beleuchtet werden, schien dies für diesen Zweck kein sinnvoller Ansatz zu sein.
Die *Risikoerfassung* erfolgte aufbauend auf den Ausführungen aus Kapitel B zu den rechtlichen Unsicherheiten, welche sich aus der Umsetzung des HinSchG für Unternehmen ergeben. So wurden die Risiken zunächst je Themengebiet aus Kapitel B erfasst, inhaltlich konkretisiert und ergänzt. An dieser

[265] Vgl. Kneisel, 2017, S. 257ff.

Stelle wäre eine ausschließliche Risikoidentifizierung anhand der vier klassischen Perspektiven der BSC nicht sinnvoll gewesen, da die Kategorien aus Kapitel B wie bereits beschrieben schon bestanden und ohne eine Umstellung der Denkweise erweitert werden konnten. Dabei war es sinnvoll die Leitfragen und Inhalte der Risiko-BSC im Hinterkopf zu behalten und an passender Stelle einfließen zu lassen. Eine zusätzliche *tabellarische Aufzählung* der Risiken je nach Themengebiet schien an dieser Stelle sinnvoll, siehe Tabellen 3 bis 5. Der Vorteil einer solchen zusätzlichen Tabelle als Zwischenschritt war die Möglichkeit zur Vorsortierung bzw. Aggregierung der Risiken.

Nachdem *Risikocluster* gebildet wurden, konnte man die Risiken den vier *Perspektiven* der Risiko-BSC zuordnen, wodurch man eine im Vergleich zur sehr umfangreichen Tabelle einen guten Überblick über den Einfluss der Risiken aus verschiedenen Perspektiven des Unternehmens erhielt. Beachtet werden mussten hierbei sowohl die Leitfragen als auch die Inhalte der jeweiligen Perspektive. Durch die vier Betrachtungsweisen – Finanzperspektive, Kundenperspektive, interne (Prozess-)Perspektive und Innovations- und Lernperspektive – entstand ein guter Überblick über die Risikoausbreitung über die verschiedenen Unternehmensbereiche und deren Einflüsse. Gerade die Anpassung der Leitfrage der Kundenperspektive im Gegensatz zu der der klassischen BSC war an dieser Stelle notwendig. Die „Kunden“ der Compliance-Abteilung gleichen nicht den klassischen Kunden des Unternehmens. Die Unterteilung in Unternehmensleitung, Betriebsrat, Mitarbeiter / hinweisgebende Personen / betroffene Personen und Externe war hilfreich, um die verschiedenen Stakeholder im Hinweisgeberprozess ausfindig zu machen und detaillierte Auswirkungen auf die Beziehung und Zusammenarbeit herausarbeiten zu können. Auch die Änderung der finanziellen Perspektive zur Beachtung der Einhaltung des Budgets war erforderlich, da der Compliance-Abteilung für ihre Tätigkeiten in der Regel ein jährliches Budget zur Verfügung gestellt wird, welches eingehalten werden sollte. Durch die Betrachtung der Risiken aus der interne (Prozess-)Perspektive konnte man erkennen, welche prozessualen Schritte und Handlungen potenzielle Risiken bergen und kann in Verbindung mit der Innovations- und Lernperspektive die Effektivität des Hinweisgebersystems als Teil des Compliance-Management-Systems

stärken. Durch die Anwendung der Risiko-BSC erhält man also einen Überblick über die Berührungspunkte verschiedener Unternehmensbereiche mit der Compliance-Abteilung oder mit Bezug zum Hinweisgebersystem.

Die *Ursache-Wirkungsbeziehu*ng der klassischen BSC kann gut auf die Risiko-BSC zum HinSchG übertragen werden. Aus einer Ineffektivität des Hinweisgebersystems und der negativen Wahrnehmung dessen und der Compliance-Mechanismen allgemein innerhalb der Belegschaft können Verbesserungen der internen Prozesse, Entscheidungen und Handlungen vorgenommen werden. Dadurch könnte sich das Verhältnis zu und die Zusammenarbeit mit den in der Kundenperspektive genannten Stakeholdern verbessern. Am Ende dieser Kette steht die finanzielle Perspektive, durch deren Sicht das Budget eingehalten werden muss.

An wenigen Stellen gestaltete sich die *Einordnung* unter die jeweiligen Perspektiven schwierig. Beispielsweise bei der Zuordnung der Schadenersatzansprüche und Geldbußen aus der DSGVO und dem BDSG, die Ordnungs- und/oder Zwangsgeldzahlungen gem. BetrVG und den Sanktionen aus dem HinSchG. Die Risiken stehen zum einen in Verbindung mit der Beziehung zu den verschiedenen Stakeholdern aus der Kundenperspektive. Allerdings entstehen hier auch finanzielle Risiken. So wurden diese Risiken zwar in der Kundenperspektive als Störfaktor in der Beziehung und Zusammenarbeit erwähnt, doch das größere Risiko scheint auf der finanziellen Ebene zu bestehen. *Mehrfachnennungen* bei der Zuordnung dieser Risiken ließen sich nicht vermeiden. Auch beim Risiko der Ineffektivität des Hinweisgebersystems bestand dieses Problem. Zum einen hat diese eine Berührung mit internen Prozessen, Entscheidungen und Handlungen, zum anderen aber auch ihre Daseinsberechtigung in der Innovations- und Lernperspektive, um die Effektivität des CMS in der Zukunft zu steigern.

Das Konzept der klassischen BSC sieht vor, dass die Ziele in der Gesamtschau *ausgewogen* betrachtet werden sollen. Im Umgang mit Unsicherheiten aus der Umsetzung des HinSchG in Unternehmen fällt auf, dass der Finanz- und Kundenperspektive mehr Risiken zugeordnet wurden als der internen (Prozess-)Perspektive und der Innovations- und Lernperspektive.

Über eine *Veränderung der klassischen Perspektiven* zur Identifizierung und Aggregierung der Risiken aus der Umsetzung des HinSchG in Unternehmen

könnte man an dieser Stelle nachdenken. Eine Möglichkeit wäre ein Stakeholderansatz aus Sicht der Compliance-Abteilung, wobei Unternehmensleitung, Betriebsrat, Mitarbeiter, hinweisgebende Personen, betroffenen Personen, Dritte und Externe jeweils eine eigene Perspektive darstellen würden. Durch die Sicht der verschiedenen Personengruppen hätte man ebenfalls eine Gesamtschau über Compliance-Schnittstellen erhalten können. Allerdings hätten bei der Risikoidentifizierung die Leitfragen der finanziellen, internen (Prozess-) Perspektive und Innovations- und Lernperspektive nicht außer Acht gelassen werden dürfen. Dadurch scheint es doch sinnvoller innerhalb der Kundenperspektive eigene Untergruppen für die jeweiligen Stakeholder zu schaffen. Auch wäre eine solche Risiko-BSC unter Umständen sehr unübersichtlich geworden, da es statt vier Perspektiven sieben gewesen wären. Eine weitere Anpassungsmöglichkeit der Perspektiven wäre die Einteilung nach finanziellen, technischen, rechtlichen und strategischen Risiken gewesen. Hierbei hätten aber die Leitfragen der klassischen Perspektiven sowie die Sichtweisen der verschiedenen Stakeholder ebenfalls nicht vernachlässigt werden dürfen. So scheint es hinsichtlich der Gesamtschau über das Unternehmen sinnvoller an den ursprünglichen Perspektiven der klassischen BSC festzuhalten.

Als separates Instrument zur *Risikoidentifikation und -analyse* bietet sich die Risiko-BSC in diesem Anwendungsbeispiel nicht an. In Verbindung mit einer tabellarischen Übersicht kann sie allerdings einen Mehrwert für den Umgang mit der Risikoerfassung bieten, da sie im Gegensatz zur alleinigen Nutzung einer Tabelle einen Überblick über die Risiken aus verschiedenen Perspektiven des Unternehmens bietet, während sie durch Clusterbildung nicht so umfangreich wie die tabellarische Aufstellung ist.

Die *Risikobewertung* erfolgte anhand der qualitativen Klassifizierung der Eintrittswahrscheinlichkeiten und Schadenshöhen des jeweiligen Risikos in Form einer separaten Risikomatrix. So diente die Risiko-BSC im Anwendungsbeispiel als Grundlage der Risikobewertung und nicht als eigenes Instrument. Ein Grund hierfür ist, dass die Aufnahme der Eintrittswahrscheinlichkeit und der Schadenshöhe in die Risiko-BSC aus Abbildung 12 eine reine Auflistung dargestellt hätte. Zum anderen bietet die Risikomatrix als Instrument des Risikomanagements eine bessere Visualisierung der Risiken im Verhältnis zueinander, was durch die farbliche

Gestaltung unterstützt wird. Grundsätzlich hätte man an dieser Stelle anstatt der qualitativen Betrachtung eine quantitative erwägen können, diese bietet sich bei der Betrachtung von Risiken aus dem Compliance-Bereich aber nicht an. Die Einordnung in die jeweiligen Kategorien der Schadensschwere und Eintrittswahrscheinlichkeit erfolgte auf Grundlage eigener Erfahrung aus der beruflichen Tätigkeit im Compliance-Bereich sowie eigener Einschätzungen. Denkbar wäre an dieser Stelle auch eine Analyse verschiedener Datenquellen wie Interviews, Fragebögen o. Ä. gewesen.

Das *Ergebnis* der Risiko-BSC in Verbindung mit der Risikomatrix kann anschließend für die Risikosteuerung, -überwachung und -kommunikation verwendet werden. Dabei könnte die Risikosteuerung in Form der Definition von Maßnahmen zur Minderung jedes einzelnen aufgeführten Risikos direkt in die Risiko-BSC integriert werden. An dieser Stelle bot sich dieses Vorgehen jedoch nicht an, da die Maßnahmen individuell auf das betroffene Unternehmen angepasst sein sollten und hierfür mangels eines konkret ausgewählten Unternehmens keine Informationen zu Größe, Mitarbeiteranzahl, Wirtschaftszweig und bestehendem Hinweisgebersystem vorlagen.

Abschließend lässt sich feststellen, dass die Risiko-BSC in Verbindung mit einer Risikomatrix als Frühwarnsystem für möglichen Risiken dienen kann. Eine Tabelle kann eine Hilfestellung bei der Sortierung und dem Clustern der Risiken bieten.

IV. Zwischenergebnis

Eine BSC kann im Risikomanagement auf verschiedene Arten zur Anwendung kommen. Am Beispiel von Risiken aus dem Compliance-Bereich wurde festgestellt, dass die Anwendung einer separaten Risiko-BSC sinnvoll ist. Die Nutzung einer Risiko-BSC wurde im Umgang mit Risiken, welche Unternehmen in Zusammenhang mit der Umsetzung des HinSchG betreffen könnten, erprobt.

Zusammenfassend lässt sich festhalten, dass sich dieser Ansatz durchaus zur Risikoidentifikation und -analyse eignet. Weiter kann die Risiko-BSC unter Zuhilfenahme einer Risikomatrix als Grundlage für die Risikobewertung dienen. Zusammen mit dieser könnte die Risiko-BSC im Anschluss für die Risikosteuerung, -überwachung und -kommunikation verwendet werden und als Entscheidungshilfe im Umgang mit den herausgearbeiteten Risiken fungieren.

D. Handlungsempfehlungen für Unternehmen

Aus den Erkenntnissen der vorhergehenden Kapitel lässt sich zusammenfassen, dass die Umsetzung des HinSchG in Unternehmen mit verschiedensten Risiken einhergehen kann. Aber schon bevor das HinSchG in Kraft tritt, ist es empfehlenswert sich mit seinen Inhalten vertraut zu machen.

In vielen Unternehmen besteht bereits im Rahmen eines effektiven CMS ein Hinweisgeberschutzsystem, welches in Anbetracht der Anforderungen des HinSchG eine Überprüfung und ggf. Anpassung durchlaufen sollte.

Eine Pflicht zur Einrichtung interner Meldestellen geht aus § 12 HinSchG hervor. So haben Beschäftigungsgeber gem. § 12 Abs. 1 HinSchG dafür zu sorgen, dass bei ihnen mindestens eine Stelle für interne Meldungen eingerichtet ist und betrieben wird, an die sich Beschäftigte wenden können. Betroffen von dieser Verpflichtung sind gem. § 12 Abs. 2 HinSchG Beschäftigungsgeber mit jeweils in der Regel mindestens 50 Beschäftigten. Gem. § 42 HinSchG können sich juristische Personen gem. § 12 Abs. 1 HinSchG mit 50 bis 249 Arbeitnehmern mit der Einrichtung oder Anpassung des Hinweisgebersystems bis zum 17.12.2023 Zeit lassen. Unabhängig von der Beschäftigtenanzahl sind gem. § 12 Abs. 3 HinSchG Unternehmen aus bestimmten Sektoren zur Einrichtung einer internen Meldestelle verpflichtet.

Neben der Zuordnung der Aufgaben einer internen Meldestelle zur vorgesehenen Abteilung oder den jeweiligen Arbeitnehmenden sollten ggf. Schulungen zur Erlangung der notwendigen Fachkunde durchgeführt werden. Auch zum Verfahren und der Vorgehensweise bei internen Meldungen sollte man sich im Voraus Gedanken machen. Besonders sinnvoll scheint schon jetzt die vorbereitende Auseinandersetzung mit dem persönlichen und sachlichen Anwendungsbereich des HinSchG. Auch sollte man sich mit dem Repressalienbegriff, der Beweislastumkehr, den Schutzvoraussetzungen sowie der Ausgestaltung von Folgemaßnahmen wie internen Untersuchungen auseinandersetzen und ggf. Verfahrensanweisungen oder Prozessbeschreibungen erstellen. Weiter könnte man bereits jetzt Maßnahmen zur Anreizsetzung bezüglich der Wahl der internen Meldestelle vorbereiten. Besonders hinsichtlich der anonymen Hinweisgabe sollte sich zur Stärkung der Effektivität des Hinweisgebersystems bereits jetzt über technische Möglichkeiten informiert werden, obwohl die betreffenden Normen gem. § 42 Abs. 2 HinSchG erst ab

dem 1. Januar 2025 anzuwenden sind. Falls auf Konzernebene bereits ein zentrales Hinweisgebersystem genutzt wird, sollte dennoch über eine zusätzliche lokale Möglichkeit der Hinweisgabe nachgedacht werden. Zu beachten ist, dass auch eine Ressourcenteilung von nicht durch Konzernverbund verknüpfte Unternehmen gem. § 14 Abs. 2 HinSchG für juristische Personen des privaten Sektors mit 50 bis 249 Arbeitnehmern möglich ist.

Nachdenken könnte man ebenfalls über die Ausweitung des Anwendungsbereichs auf die Meldung interner Regelverstöße und eine damit einhergehende Selbstverpflichtung zur Beachtung der Schutzvorschriften des HinSchG, da damit die Effektivität des Hinweisgebersystems gesteigert werden könnte.

Um mit einigen aus der Verabschiedung des HinSchG folgenden rechtlichen Unsicherheiten und damit verbundenen Risiken besser umgehen zu können, sollten Unternehmen die Anwendung von Risikomanagementinstrumenten in Erwägung ziehen. Als Instrument zur Risikoidentifikation und -analyse eignet sich eine Risiko-BSC, welche zur Bewertung der Risiken um eine Risikomatrix erweitert werden kann. Die Kombination beider Instrumente ebnet den Weg, um bereits im Voraus geeignete Maßnahmen zur Risikominimierung definieren zu können.

E. Zusammenfassung

Diese Masterarbeit hat aufgezeigt, dass die Umsetzung des HinSchG in Unternehmen mit rechtlichen Unsicherheiten und daraus resultierenden Risiken verbunden ist. Die klassische BSC kann durch wenige Anpassungen zu einem Instrument des Risikomanagements weiterentwickelt werden und im Umgang mit den genannten Risiken eine Hilfestellung darstellen. Dabei kann sie als Instrument zur Risikoidentifikation und -analyse und als Grundlage für die Risikobewertung mithilfe einer Risikomatrix dienen.

Da mit einer baldigen Verabschiedung des HinSchG zu rechnen ist, ist es bereits jetzt für die von einer Einrichtungspflicht interner Meldestellen betroffenen Unternehmen sinnvoll, sich mit den Inhalten des Gesetzes und den daraus resultierenden Risiken zu beschäftigen. Neben der reinen Lektüre der Normen wird eine Risikoanalyse empfohlen, bei der eine Risiko-BSC eine Hilfestellung sein kann.

Auch für Unternehmen, welche nicht von der Einrichtungspflicht einer internen Meldestelle gem. HinSchG betroffen sind, könnte das Befassen mit den Inhalten und Risiken durchaus sinnvoll sein. Im Rahmen eines effektiven CMS ist die Implementierung eines Hinweisgebersystems unabdingbar, sofern den hinweisgebenden Personen dabei ausreichend Schutz gewährt wird.

Literaturverzeichnis

Altenbach, Thomas / Dierkes, Kevin: EU-Whistleblowing-Richtlinie und DSGVO. CCZ 2020, S. 126 - 132.

Bayreuther, Frank: Whistleblowing und das neue Hinweisgeberschutzgesetz. NZA-Beilage, 2022, S. 20 - 29.

Behringer, Stefan: Compliance kompakt. Best Practice im Compliance-Management. 4. Auflage. 2018.

Brauweiler, Hans-Christian: Risikomanagement in Unternehmen. Ein grundlegender Überblick für die Management-Praxis. 2. Auflage. 2019.

Brühwiler, Bruno: Unternehmensweites Risk Management als Frühwarnsystem – Methoden und Prozesse für die Bewältigung von Geschäftsrisiken in integrierten Managementsystemen. 2001.

Buchert, Christoph: Der Irrweg der EU-Kommission – Zu den Überlegungen über die Einführung einer staatlichen Whistleblower-Prämie. CCZ 2013, S. 144 - 149.

Bürkle, Jürgen: Zur Unionsrechtskonformität zentraler Konzernmeldestellen für Hinweisgeber. CCZ 2022, S. 335 - 340.

Bundesministerium der Justiz: Referentenentwurf – Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden. 13.04.2022. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Hinweisgeberschutz.pdf?__blob=publicationFile&v=1. Zuletzt aufgerufen am 03.04.2023.

Bundesrechtsanwaltskammer: Stellungnahme zum HinSchG-RefE. 17.05.2022. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2022/Downloads/0517_Stellungnahme_BRAK_HinSchG-E.pdf;jsessionid=FAFC670591CF5A973D0F1720DC3157AC.1_cid289?__blob=publicationFile&v=2. Zuletzt aufgerufen am 03.04.2023.

Bundesregierung: Formulierungshilfe zum Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden. 14.03.2023. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/FH_HinSchG.pdf?__blob=publicationFile&v=1. Zuletzt aufgerufen am 03.04.2023.

Bundesregierung: Gesetz zum Hinweisgeberschutz. Besserer Rechtsschutz für „Whistleblower". 14.03.2023. https://www.bundesregierung.de/breg-de/suche/hinweisgeberschutz-2064178. Zuletzt aufgerufen am 03.04.2023. (zitiert als Bundesregierung, 2023, Online-Artikel)

Bundesregierung: Regierungsentwurf – Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden. 27.07.2022. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Hinweisgeberschutz.pdf?__blob=publicationFile&v=2. Zuletzt aufgerufen am 03.04.2023.

Bundesregierung: Regierungsentwurf – Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft. 2020. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Staerkung_Integritaet_Wirtschaft.pdf;jsessionid=AAADBAD578959C7DF72719C5C6E6C776.2_cid297?__blob=publicationFile&v=2. Zuletzt aufgerufen am 03.04.2023.

Bundesverband der Compliance Manager: Stellungnahme zum HinSchG-RefE. 11.05.2022. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2022/Downloads/0511_Stellungnahme_BCM_HinSchG-E.pdf;jsessionid=D04DEC7C1B7E362C8BE0AE42695D7BC5.2_cid334?__blob=publicationFile&v=4. Zuletzt aufgerufen am 03.04.2023.

Bundesverband der Deutschen Industrie: Stellungnahme zum HinSchG-RefE. 11.05.2022. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2022/Downloads/0511_Stellungnahme_BDI_HinSchG-E.pdf;jsessionid=D04DEC7C1B7E362C8BE0AE42695D7BC5.2_cid334?__blob=publicationFile&v=4. Zuletzt aufgerufen am 03.04.2023.

Bundesverband für Unternehmensjuristen: Stellungnahme zum HinSchG-RefE. 11.05.2022. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2022/Downloads/0511_Stellungnahme_BUJ_HinSchG-E.pdf;jsessionid=FAFC670591CF5A973D0F1720DC3157AC.1_cid289?__blob=publicationFile&v=2. Zuletzt aufgerufen am 03.04.2023.

Colneric, Ninon: Stellungnahme zum HinSchG-RefE. 06.05.2022. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2022/Downloads/0506_Stellungnahme_Prof._Dr._Ninon_Colneric_HinSchG-E.pdf;jsessionid=D04DEC7C1B7E362C8BE0AE42695D7BC5.2_cid334?__blob=publicationFile&v=2. Zuletzt aufgerufen am 03.04.2023.

Colneric, Ninon / Gerdemann, Simon: Die Umsetzung der Whistleblower-Richtlinie in deutsches Recht. Rechtsfragen und rechtspolitische Überlegungen. HSI-Schriftenreihe, Band 34. 2020.

Datenschutzkonferenz: Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz. 2018. https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf. Zuletzt aufgerufen am 03.04.2023.

Degenhart, Maximilian / Dziuba, Anne: Die EU-Whistleblower-Richtlinie und ihre arbeitsrechtlichen Auswirkungen. BB 2021, S. 570 - 574.

Deutscher Anwaltsverein: Stellungnahme zum HinSchG-RefE. 17.05.2022. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2022/Downloads/0517_Stellungnahme_DAV_HinSchG-E.pdf;jsessionid=FAFC670591CF5A973D0F1720DC3157AC.1_cid289?__blob=publicationFile&v=3. Zuletzt aufgerufen am 03.04.2023.

Deutsches Institut für Compliance: Stellungnahme zum HinSchG-RefE. 11.05.2022. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2022/Downloads/0511_Stellungnahme_DICO_HinSchG-E.pdf;jsessionid=FAFC670591CF5A973D0F1720DC3157AC.1_cid289?__blob=publicationFile&v=2. Zuletzt aufgerufen am 03.04.2023.

Dillerup, Ralf / Stoi, Roman: Unternehmensführung. 4. Auflage. 2013.

Dilling, Johannes: Der Schutz von Hinweisgebern und betroffenen Personen nach der EU-Whistleblower-Richtlinie. CCZ 2019, S. 214 -224.

Dilling, Johannes: Der Referentenentwurf zum Hinweisgeberschutzgesetz – Steine statt Brot für Whistleblower und betroffenen Personen. CCZ 2021, S. 60 - 67.

Dilling, Johannes: Cat's Gold-Plating – Der neue Referentenentwurf zum Hinweisgeberschutzgesetz. CCZ 2022, S. 145 - 151.

Dohrmann, Vanessa: Die geplante Umsetzung der EU-Whistleblower-Richtlinie aus arbeitsrechtlicher Sicht. RdA 2021, S. 326 - 332.

Dzida, Boris / *Granetzny*, Thomas: Die neue EU-Whistleblowing-Richtlinie und ihre Auswirkungen auf Unternehmen. NZA, 2020. S. 1201 - 1207.

Engels, Hannah: Whistleblower-Schutz in Unternehmen. ARP 2020, S. 20 - 23.

Europäische Kommission: Minutes of the fifth meeting of the Commission expert group on Directive (EU) 2019/1937. 14.06.2021 https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=28015&fromExpertGroups=true. Zuletzt aufgerufen am 03.04.2023.

European Center for Whistleblower Rights: Stellungnahme zum HinSchG-RefE. 06.05.2022. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2022/Downloads/0506_Stellungnahme_ECWR_HinSchG-E.pdf;jsessionid=D04DEC7C1B7E362C8BE0AE42695D7BC5.2_cid334?__blob=publicationFile&v=3. Zuletzt aufgerufen am 03.04.2023.

Europäischer Datenschutzbeauftragter: Guidelines on processing personal information within a whistleblowing procedure. 2016. https://edps.europa.eu/sites/edp/files/publication/16-07-18_whistleblowing_guidelines_en.pdf. Zuletzt aufgerufen am 03.04.2023.

Fleischer, Holger / Schmolke, Klaus Ulrich: Finanzielle Anreize für Whistleblower im Europäischen Kapitalmarktrecht? Rechtspolitische Überlegungen zur Reform des Marktmissbrauchregimes. NZG 2012, S. 361 - 368.

Forst, Gerrit: Die Richtlinie der Europäischen Union zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (Whistleblowing-Richtlinie). EuZA 2020, S. 283 - 302.

Franzen, Martin / Gallner, Inken / Oekter, Hartmut (Hrsg.): Kommentar zum europäischen Arbeitsrecht. 4. Auflage. 2022. C. H. Beck, München. (zitiert als Bearbeiter in Franzen/Gallner/Oetker)

Freidank, Carl-Christian: Integration eines Hinweisgebersystems in die Corporate Governance von Aktiengesellschaften. DStR 2022, S. 1871 - 1875.

Fuhlrott, Michael / Henckel, Christoph: Hinweisgeberschutzgesetz: Handlungsbedarf für Unternehmen und Personalabteilungen. ArbRAktuell 2022, S. 441 - 445.

Gerdemann, Simon: Neuer Entwurf für ein Hinweisgeberschutzgesetz. Auf Konfrontationskurs zu EU-Kommission und Koalitionsvertrag. ZRP 2022, S. 98 - 101. (zitiert als Gerdemann, 2022/1)

Gerdemann, Simon: Stellungnahme zum HinSchG-RefE. 11.05.2022. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2022/Downloads/0511_Stellungnahme_gerdemann_HinSchG-E.pdf;jsessionid=E18EB3FEB01D05273460230513A1EF85.2_cid289?__blob=publicationFile&v=2. Zuletzt aufgerufen am 03.04.2023. (zitiert als Gerdemann, 2022/2)

Gerdemann, Simon: Referentenentwurf für ein deutsches Hinweisgeberschutzgesetz. ZRP 2021, S. 37 - 39. (zitiert als Gerdemann, 2021)

Gilles, Michael: Balanced Scorecard als Konzept zur strategischen Steuerung von Unternehmen. Europäische Hochschulschriften. 2002.

Glage, Dietmar / Grötzner, Marc: § 14 Unternehmensrisiken und Risikomanagement. In *Hauschka, Christoph / Moosmayer, Klaus / Lösler, Thomas:* Corporate Compliance. Handbuch der Haftungsvermeidung in Unternehmen. 3. Auflage. 2016.

Gleißner, Werner / Romeike, Frank: Risiko und Balanced Scorecard. In: *Gleißner,* Werner / *Romeike, Frank* (Hrsg.): Praxishandbuch Risikomanagement. Konzepte – Methoden – Umsetzung. 2015, S. 546 - 560.

Gleißner, Werner: Integratives Risikomanagement – Schnittstellen zu Controlling, Compliance und Interner Revision. Controlling 4/2020, S. 23 - 29.

Granetzny, Thomas / Krause Melena: Was kostet ein gutes Gewissen? – Förderung von Whistleblowing durch Prämien nach US-Vorbild? CCZ 2020, S. 29 - 36.

Hamm-Düppe, Yvonne: EU-Hinweisgeberrichtlinie: Sind die praktischen Umsetzungsherausforderungen lösbar? – Ein Praxisbericht zur Umsetzung der EU-Hinweisgeberrichtlinie im Konzern aus deutscher Sicht. CCZ 2022, S. 409 – 411.

Hauschka, Christoph: § Einführung. In *Hauschka, Christoph / Moosmayer, Klaus / Lösler, Thomas:* Corporate Compliance. Handbuch der Haftungsvermeidung in Unternehmen. 3. Auflage. 2016.

Heimer, Sebastian: Die Balanced Scorecard als Instrument zur Unterstützung des Risikomanagements. In: *Höschler, Reinhold (Hrsg.):* Studien zum Finanz-, Bank- und Versicherungsmanagement Band 13. 2007. https://kluedo.ub.uni-kl.de/frontdoor/deliver/index/docId/4289/file/_LFF+Studien+Band+13+-+Die+Balanced+Scorecard+als+Instrument+zur+Unterst%c3%bctzung+des+Risikomanagements+ohne+Schutz.pdf. Zuletzt aufgerufen am 03.04.2023

Henschel, Thomas / Heinze, Ilka: Governance, Risk und Compliance im Mittelstand. Praxisleitfaden für gute Unternehmensführung. 2016.

Henseler, Jörg / Jonen, Andreas / Lingnau, Volker: Die Rolle des Controllings bei der Ein- und Weiterführung der Balanced Scorecard. Eine empirische Untersuchung. In: *Lingnau, Volker. (Hrsg.):* Beiträge der Controlling Forschung, Nr. 7. 2. Auflage. 2006.

Horváth & Partners (Hrsg.): Balanced Scorecard umsetzen. 4. Auflage. 2007. Schäffer-Poeschel, Stuttgart.

Hunziker, Stefan / Fallegger, Marcel / Jovic, Kristijan: Risiko-Management im Führungssystem einbinden. Controlling & Management Review 9/2018, S. 54 - 59.

IDW: IDW Prüfungsstandard 980: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen. 2011. (zitiert als IDW PS 980)

ISO: DIN ISO 37301: Compliance-Managementsysteme – Anforderungen mit Anleitung zur Anwendung. 2020. (zitiert als ISO 37301)

Kaplan, Robert / Norton, David: Balanced Scorecard. Strategien erfolgreich umsetzen. 2018. Schäffer-Poeschel, Stuttgart.

Kappen, Stefanie / Cho, Mina / Gärtner, Bernhard: Konzernlösung des HinSchG-E – unionsrechtswidrig? CB 2022, S. 237 - 242.

Klafki, Anika: Risiko und Recht. Risiken und Katastrophen im Spannungsfeld von Effektivität, demokratischer Legitimation und rechtsstaatlichen Grundsätzen am Beispiel von Pandemien. 2017.

Kneisel, Katharina: Nutzung einer Compliance-Scorecard. Putting Compliance Strategy Into Action. ZRFC 6/2017, S. 257.

Krisper, Georg: Die Integration von Risikomanagement in eine Balanced Scorecard. Masterarbeit eingereicht am Institut für Unternehmensrechnung und Controlling Karl-Franzens-Universität Graz bei Alfred Wagenhofer. 2009. https://unipub.uni-graz.at/obvugrhs/content/titleinfo/245703?lang=en. Zuletzt aufgerufen am 04.03.2022.

Leyens, Patrick C.: Selbstbindungen an untergesetzliche Verhaltensregeln. AcP 2015, S. 611 - 654.

Löber, Nils: Strategische Planung und Umsetzung des klinischen Risikomanagements. In: *Becker, Andreas*: Reader Risikomanagement im Krankenhaus. 2016, S. 15 - 33.

Lüneborg, Cäcilie: Neue Pflichten zur Einrichtung von Hinweisgebersystemen – Integrierte Umsetzung in der Unternehmenspraxis. DB 2022, S. 375 - 384. (zitiert als Lüneborg, 2022/1)

Lüneborg, Cäcile: Der Regierungsentwurf des Hinweisgeberschutzgesetzes: Kein großer Wurf. NZG 2022, S. 1273. (zitiert als Lüneborg, 2022/2)

Metzner, Isabel / Gloeckner, Felix: „Reality Check" der EU-Whistleblower Richtlinie – Ist die Einführung eines lokalen Hinweisgebersystems wirklich erforderlich? CCZ 2021, S. 256 - 259.

Metzner, Isabel / Hustert, Sven / Hommel, Ulf: Praktische Herausforderungen im Konzern durch die EU-Hinweisgeberrichtlinie. CCZ 2022, S. 117 - 119.

Nießen, Tobias: Neuerung beim Hinweisgeberschutz. RFamU 2022, S. 399 - 404.

Otremba, Stefan: Integriertes Risikomanagement. Die erfolgreiche Integration und Weiterentwicklung des Risikomanagements. 2019. https://kpmg.com/de/de/home/themen/2019/06/integriertes-risikomanagement.html. Zuletzt aufgerufen am 03.04.2023.

Pampel, Jochen / Krolak, Thomas: § 15 Risikomanagement durch Controlling. In *Hauschka, Christoph / Moosmayer, Klaus / Lösler, Thomas:* Corporate Compliance. Handbuch der Haftungsvermeidung in Unternehmen. 3. Auflage. 2016.

Pauthner, Jürgen / Stephan, Hans-Jürgen: § 15 Risikomanagement durch Controlling. In*: Hauschka, Christoph / Moosmayer, Klaus / Lösler, Thomas:* Corporate Compliance. Handbuch der Haftungsvermeidung in Unternehmen. 3. Auflage. 2016.

Romeike, Frank: Risikomanagement. Studienwissen kompakt. 2018. Springer / Gabler, Wiesbaden.

Schmola, Gerald: Grundlagen und Instrumente des Risikomanagements. In: *Schomla, Gerald / Rapp, Boris (Hrsg.):* Compliance, Governance und Risikomanagement im Krankenhaus. Rechtliche Anforderungen – Praktische Umsetzung – Nachhaltige Organisation. 2016, S. 289 - 340.

Siemes, Christiane: Der Schutz verbundener Personen nach der EU-Whistleblowing-Richtlinie und seine Umsetzung ins deutsche Recht. CCZ 2022, S. 7 - 13.

Simitis, Spiros / Hornung, Gerrit / Spiecker gen. Döhmann, Indra: Datenschutzrecht. DSGVO mit BDSG. 2019. (zitiert Simitis/Hornung/Spiecker gen. Döhmann/Verfasser)

Schmolke, Klaus Ulrich: Die neue Whistleblower-Richtlinie ist da! Und nun? Zur Umsetzung der EU-Richtlinie zum Schutz von Hinweisgebern in das deutsche Recht. NZG 2020, S. 5 - 12.

Steinhauser, Rut / Saalwächter-Hirsch, Caroline / Trouvain, Till: Das deutsche Hinweisgeberschutzgesetz – Was lange währt, wird endlich gut? ESG 2023, S. 329 – 333.

Taschke, Jürgen / Pielow, Tobias / Volk, Eva: Die EU-Whistleblowing-Richtlinie – Herausforderungen für die Unternehmenspraxis. NZWiSt 2021, S. 85 - 92.

Teichmann, Ulrich / Erkens, Nils: Controllingintegriertes Risikomanagement nach KonTraG mit der Balanced Scorecard – am Beispiel der Wohnungswirtschaft. Dortmunder Diskussionsbeiträge zur Wirtschaftspolitik Nr. 101 2000, S. 28ff.

Thüsing, Gregor / Forst, Gerrit: Beschäftigtendatenschutz und Compliance. 3. Auflage.2021.

Transparency International: Stellungnahme zum HinSchG-RefE. 10.05.2022. https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2022/Downloads/0510_Stellungnahme_Transparency_Inter_HinSchG-E.pdf;jsessionid=D04DEC7C1B7E362C8BE0AE42695D7BC5.2_cid334?__blob=publicationFile&v=2. Zuletzt aufgerufen am 03.04.2023.

Transparency International: Assessing Whistleblowing Legislation: Methodology and guidelines for assessment against the EU Directive and best practice. 2020. https://images.transparencycdn.org/images/2020_Toolkit_AssessingWhistleblowingLegislation_EN.pdf. Zuletzt aufgerufen am 03.04.2023.

Tüllner, Jörg: Integration von Governance, Risikomanagement und Compliance. ZCG 3/2012, S. 118 - 121.

Vetter, Eberhard: Compliance in Unternehmen. In: *Wecker, Gregor / Ohl, Bastian (Hrsg.):* Compliance in der Unternehmenspraxis. Grundlagen, Organisation und Umsetzung. 2013, S. 1 - 18.

Wagner, Andreas: The Balanced Scorecard as a Tool for Value Management in Banks. In: *Schuster, Leo (Hrsg.):* Shareholder Value Management in Banks. 2000, S. 82 - 95.

Wahl, Rainer/Appel, Ivo: Prävention und Vorsorge. Von der Staatsaufgabe zur rechtlichen Ausgestaltung. In: *Wahl, Rainer (Hrsg.):* Prävention und Vorsorge. Von der Staatsaufgabe zu den verwaltungsrechtlichen Instrumenten. 1995, S. 1 – 216.

Weber, Beatrix: Rechtliche Herausforderungen durch Compliance. In: Schomla, Gerald / Rapp, Boris (Hrsg.): Compliance, Governance und Risikomanagement im Krankenhaus. Rechtliche Anforderungen – Praktische Umsetzung – Nachhaltige Organisation. 2016, S. 3 - 24.

Weber, Jürgen / *Weißenberger*, Barbara / *Liekweg,* Armin: Risk Tracking and Reporting: Unternehmerisches Chancen- und Risikomanagement nach dem KonTraG. In: Schriftenreihe Advanced Controlling, Band 11/1999.

Wengert, Holger / Schittenhelm, Frank Andreas: Corporate Risk Management. 2013.

Withus, Karl-Heinz: Betriebswirtschaftliche Grundsätze für Compliance-Management-Systeme. Struktur, Elemente und Ausgestaltung nach IDW PS 980. 2014.

Zimmer, Mark / *Schwunk*, Benita: Hilfe für Hinweisgeber – Beweislastumkehr nach § 36 II HinSchG-RegE. NZA 2022, S. 1167 - 1172.

Zimmer, Mark / Humphrey, Katharina: Petzen? Ja, bitte! Meldesysteme nach der Whistleblower-Richtlinie der EU. BB 2022, S. 372 - 376.

Zimmermann, Gebhard / *Jöhnk, Thorsten*: Risikomanagement mit der Balanced Scorecard – ein Überblick. Zeitschrift für das gesamte Kreditwesen 17/2002, S. 57 - 60. https://www.econbiz.de/Record/risikomanagement-mit-der-balanced-scorecard-ein-%C3%BCberblick-zimmermann-gebhard/10001692543. Zuletzt aufgerufen am 03.04.2023.

Eidesstattliche Erklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe; die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde nach meiner besten Kenntnis bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Mering, 05. April 2023 Unterschrift