Lizenziert für .
Die Inhalte sind urheberrechtlich geschützt.

ZfRM

03.22

3. Jahrgang
Juni 2022
S. 57 – 84

# Zeitschrift für RISIKOMANAGEMENT

Praxiswissen risikobasierte Unternehmensführung

www.ZfRMdigital.de

## Umgang mit Klimarisiken

### Wie sich Nachhaltigkeitsziele umsetzen lassen

**Fachbeirat:**

**Dr. Oliver Bungartz,**
RSM Risk Consulting Germany GmbH & Co. KG, Leiter „Risk Advisory"

**Prof. Dr. Peter Fissenewert,**
Buse Heberer Fromm, Partner

**Prof. Dr. Werner Gleißner,**
FutureValue Group AG, Vorstand, Technische Universität Dresden

**Prof. Dr. Ute Vanini,**
Fachhochschule Kiel

**Andreas Wermelt,**
Deloitte GmbH, Partner

ESV ERICH SCHMIDT VERLAG

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2022 (https://zfrmdigital.de) - 20.06.2022 14:57

Lizenziert für .
Die Inhalte sind urheberrechtlich geschützt.



# Hinweisgeberschutz: Gesetzentwurf liegt vor

## EU-Richtlinie gut umgesetzt, aber noch deutliche Lücken

Interview mit Prof. Dr. Peter Fissenewert

**Prof. Dr. Peter Fissenewert**
Rechtsanwalt und Partner der Kanzlei BUSE am Standort Berlin

Whistleblowing gewinnt an Bedeutung. Hinweisgebern soll besonderer Schutz zukommen, damit sie rechtliche Verstöße in und von Organisationen ohne negative berufliche oder persönliche Konsequenzen melden können. Die EU-Staaten hatten deshalb Ende 2019 eine Whistleblower-Richtlinie verabschiedet. Jetzt hat die Bundesregierung einen Referentenentwurf für die Umsetzung in nationales Recht veröffentlicht. Rechtsanwalt Prof. Dr. Peter Fissenewert erörtert im Interview mit Chefredakteur Wolfhart Fabarius Details des Gesetzentwurfs und zeigt auf, worauf es für das Risikomanagement ankommt.

**Wie bewerten Sie den Referentenentwurf des Bundesjustizministeriums insgesamt? Ist die entsprechende EU-Richtlinie nach Ihrer Einschätzung sinnvoll und angemessen umgesetzt worden?**

**Peter Fissenewert:** Es ist gut, dass nun wieder ein Referentenentwurf vorgelegt wurde und dies auch schon in relativ kurzer Zeit nach der Koalitionsbildung. Der Referentenentwurf hat gute und vielversprechende Ansätze und hat die EU-Richtlinie auch in vielen Punkten gut umgesetzt. Gleichwohl gibt es noch Diskussionsbedarf.

**In welcher Hinsicht? Was würden Sie gegenüber dem vorliegenden Entwurf noch geändert sehen?**

Der Gesetzesentwurf enthält deutliche Lücken. So sind weder interne noch externe Meldestellen nach dem Entwurf verpflichtet, Verfahren für anonyme Meldungen vorzuhalten oder solche Meldungen überhaupt zu bearbeiten. Die Begründung hierfür soll sein, das neue Hinweisgeberschutzsystem nicht zu überlasten und zunächst erste Erfahrungen abzuwarten. Aus meiner persönlichen Erfahrung belasten anonyme Hinweise aber keineswegs irgendein System, sondern sind eine wunderbare Handreichung an die Mitarbeiterinnen und Mitarbeiter, sich tatsächlich anonym melden zu können. Und diese anonyme Meldung muss selbstverständlich auch bearbeitet werden. Bedauerlich finde ich auch, dass hier nur bestimmte Rechtsverstöße geschützt werden, etwa straf- oder bußgeldbewährte Verstöße, nicht aber etwaige Richtlinien, erst recht nicht unternehmensinterne Richtlinien, obwohl dies doch so wichtig wäre. Das bekannteste Beispiel hierfür sind die Missstände in der Pflege und die wenigen damit einhergehenden Enthüllungen von überlasteten Mitarbeitern. Das zeigt, dass nicht jedes Fehlverhalten ein Rechtsverstoß ist, wie er vom Gesetz gefordert wird.

**Welches sind die zentralen Punkte im Gesetz, die das Risikomanagement unbedingt kennen und beachten sollte?**

Verstöße gegen das Hinweisgeberschutzgesetz bergen erhebliche Risiken in sich, sowohl für die Verantwortlichen als auch für das Unternehmen. Vor diesem Hintergrund ist es unabdingbar, dass die korrekte Einrichtung und Zurverfügungstellung der Meldesysteme ständig überprüft werden. Auch bedarf es eines strengen Risikomanagementsystems, insbesondere im Hinblick auf die Nichtbehinderung von Hinweisgebern in jeglicher Hinsicht. Hier muss ein engmaschiges Netz aus zulässiger Überprüfung des Ob und

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2022 (https://zfrmdigital.de) - 20.06.2022 14:57

Lizenziert für .
Die Inhalte sind urheberrechtlich geschützt.



Wann in zeitlicher Hinsicht ebenso erfolgen wie in sachlicher Hinsicht.

**Wie sollte das Risikomanagement das interne Meldesystem ausgestalten, damit Whistleblower hinreichend Anreiz haben, Meldungen intern abzugeben und sich nicht an eine externe Meldestelle zu wenden?**

Ein Meldesystem ist immer dann attraktiv, wenn es funktioniert, wenn also der Hinweisgeber einen einfachen Zugang zum System hat. Und es ist erst recht dann attraktiv für den Hinweisgeber, wenn er merkt, dass er ernst genommen und sein Hinweis schnell, nachvollziehbar und möglichst sichtbar bearbeitet wird. Der interne Meldekanal steht hier quasi in Konkurrenz zum externen Meldekanal und es muss eben für den Mitarbeiter attraktiver sein, sich intern an den Kanal zu wenden, als eben einen externen Weg zu wählen.

**Für viele Unternehmen wird das zu erheblichem Handlungsbedarf führen. Worauf wird es nun in erster Linie ankommen?**

Unternehmen, die bislang noch gar kein Hinweisgebersystem installiert haben, werden sich nun erstmals mit der Einrichtung entsprechender Meldekanäle befassen müssen. Und Unternehmen, die bereits über ein Hinweisgebersystem verfügen, werden prüfen müssen, ob dieses auch künftig die gesetzlichen Vorgaben an Meldewege, Verfahrensgrundsätze und Vertraulichkeit erfüllt. Will man vermeiden, dass Beschäftigte festgestellte Auffälligkeiten direkt an die zuständigen Behörden melden, bleibt die Einrichtung einer internen Meldestelle unumgänglich. Daher dürfte es im Interesse sämtlicher Unternehmen liegen, ein möglichst attraktives Hinweisgebersystem aufzubauen. Diejenigen Unternehmen, die bereits über ein funktionierendes Compliance-Management-System verfügen, werden auch keine Schwierigkeiten damit haben.

**Welche Mindestanforderungen bestehen für ein internes Meldesystem?**

Bei der genauen Ausgestaltung des internen Meldekanals besteht Gestaltungsspielraum. Daher würde grundsätzlich auch ein unternehmensinterner Briefkasten genügen, wobei diese Option mit Blick auf die gesetzlichen Vorgaben einen erheblichen organisatorischen Aufwand erfordert. So leicht ist es also nicht. Vor diesem Hintergrund bietet sich deshalb in erster Linie die Einrichtung einer elektronischen Meldemöglichkeit an. Zur Entgegennahme der Meldungen kann auch ein Rechtsanwalt als externer Ombudsmann beauftragt werden. In jedem Fall benötigt die betreffende Person hinreichende Kompetenzen, um die notwendige rechtliche Bewertung der Meldungen vornehmen zu können.

**Und wie genau ist nun das Meldesystem aufzusetzen?**

Die Meldewege müssen so ausgestaltet sein, dass die Hinweise in schriftlicher oder mündlicher Form erfolgen können. Außerdem soll auf Wunsch des Hinweisgebers auch eine physische Zusammenkunft innerhalb eines angemessenen Zeitrahmens ermöglicht werden. In jedem Fall muss die Vertraulichkeit des Hinweisgebers gewahrt werden. Die unterschiedlichen Meldemöglichkeiten können miteinander kombiniert werden. Das sollte abhängig sein von der Lösung, die favorisiert wird und wird im konkreten Einzelfall von der Größe und Struktur des Unternehmens abhängen.

**Gehen wir einmal davon aus, der Whistleblower hat sich aus welchen Gründen auch immer für die Nutzung eines externen Meldesystems entschieden. Was bedeutet das nun für ein Unternehmen? Inwiefern haben Unternehmen eine Chance, in so einem Fall in das Verfahren aktiv einzugreifen?**

Für ein Unternehmen ist es immer besser, wenn der interne Meldekanal genutzt wird, weil das Unternehmen schneller reagieren kann und das Problem im Haus, also ohne größere Öffentlichkeit und ohne größeres Nachfragen erledigt werden kann. Erfolgt die Meldung dann aber doch über einen externen Kanal, besteht für ein Unternehmen nur dann die Chance, in das Verfahren aktiv einzugreifen, wenn sich die externe Meldestelle wegen weiterer Aufklärungen an das Unternehmen wendet. Ansonsten sind die Eingriffsmöglichkeiten extrem beschränkt.



© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2022 (https://zfrmdigital.de) - 20.06.2022 14:57

Lizenziert für .
Die Inhalte sind urheberrechtlich geschützt.



**Welche Anforderung werden an die im Meldesystem involvierten Akteure gestellt?**

Damit die internen Meldestellen funktionsfähig sind und die notwendigen Vorkehrungen getroffen werden, um die Vertraulichkeit der Identität der von der Meldung betroffenen Person zu wahren, ist dafür Sorge zu tragen, dass die mit den Aufgaben einer internen Meldestelle beauftragten Personen über die notwendige Fachkunde zur Erfüllung aller der Meldestelle übertragenen Aufgaben verfügen. Dies kann beispielsweise durch geeignete Schulungen sichergestellt werden. In Betracht für fachkundige Personen kommen der Korruptionsbeauftragte, der Identitätsbeauftragte und der Datenschutzbeauftragte.

**Greift denn der Hinweisgeberschutz tatsächlich bei jeglicher Form von Verstößen? Oder sind ihm Grenzen gesetzt, beispielsweise bei Sicherheitsinteressen, Verschwiegenheitspflichten und Geheimhaltungspflichten?**

Das Gesetz schützt im Grundsatz nur Meldungen gegen Rechtsverstöße. Genauso wichtige andere Missstände sind nicht vom Gesetz umfasst. Vom Anwendungsbereich ausgenommen sind auch Informationen, die beispielsweise die nationale Sicherheit betreffen. Der Gesetzesentwurf sieht hier grundsätzlich einen Vorrang von Sicherheitsinteressen und von Verschwiegenheits- und Geheimhaltungspflichten, die dem Hinweisgeberschutz vorangestellt sind. Aus Gründen des Staatswohls sei die Weitergabe schutzbedürftiger Informationen unabhängig von ihrem Geheimhaltungsgrad durch Meldung oder Offenlegung nicht vom Anwendungsbereich des Gesetzes umfasst. Zum Schutz der nationalen Sicherheit und wesentlicher Sicherheitsinteressen sei es gerechtfertigt, entsprechende Informationen vor einer Weitergabe durch Meldung oder Offenlegung zu schützen. Hiervon erfasst sind insbesondere Informationen, deren Weitergabe den Bestand oder die Funktionsfähigkeit der Bundesrepublik Deutschland oder eines ihrer Bundesländer berühren können. Auch Interessen kollektiver Sicherheitssysteme können nationale Sicherheitsinteressen berühren. Ähnliches gilt für die Weitergabe schutzbedürftiger Informationen unabhängig von ihrem Geheimhaltungsgrad.

**Beschäftigte, die in einer Meldung genannt oder gar beschuldigt werden, haben einerseits gemäß Datenschutzgrundverordnung das Recht auf Information über die Zwecke der Datenverarbeitung und den Anspruch auf Auskunft über den die Person betreffenden Inhalt der Meldung. Andererseits darf die Identität des Whistleblowers gemäß Whistleblower-Richtlinie nicht offengelegt werden. Wie wird dieses Spannungsverhältnis im Gesetzentwurf gelöst?**

Die Meldestellen haben nach § 8 des Gesetzesentwurfes die Vertraulichkeit der Identität der hinweisgebenden Person zu wahren, sofern die gemeldeten Informationen Verstöße betreffen, die in den Anwendungsbereich dieses Gesetzes fallen, oder die hinweisgebende Person zum Zeitpunkt der Meldung hinreichenden Grund zu der Annahme hatte, dass dies der Fall sei. Dies ist schon eine kleine Hürde, weil der Schutz tatsächlich nur in den Fällen gewährleistet ist, die in den Anwendungsbereich dieses Gesetzes fallen. Da muss man im Zweifel einen Juristen hinzuziehen.

**Damit ein Hinweisgeberschutzsystem also wirksam und funktionstüchtig ist, muss die Identität aller von einer Meldung betroffenen Personen weitgehend geschützt werden. Wie ist das konkret gewährleistet?**

Um das Vertraulichkeitsgebot nicht zu konterkarieren, ist es erforderlich, die Ausübung bestimmter datenschutzrechtlicher Auskunfts- und Informationsrechte einzuschränken. Die Gesetzesvorlage verweist hier auf § 29 Abs. 1 BDSG. Über die dort geforderte Interessenabwägung lassen sich der erforderliche Gleichlauf zwischen dem Vertraulichkeitsschutz und datenschutzrechtlichen Informationspflichten und Auskunftsrechten herstellen. Den datenschutzrechtlich Verantwortlichen treffen keine Informationspflichten, soweit dies Informationen offenbaren würde, die ihrem Wesen nach geheim gehalten werden müssen. War das Datenschutzrecht bislang schon kompliziert, wird es in diesen Fällen noch komplizierter.

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2022 (https://zfrmdigital.de) - 20.06.2022 14:57

Lizenziert für .
Die Inhalte sind urheberrechtlich geschützt.



**In welchen Ausnahmefällen darf die Identität des Hinweisgebers genannt werden?**

Personen, die vorsätzlich oder grob fahrlässig unrichtige Informationen über Verstöße melden, sind nicht vom Hinweisgeberschutzgesetz geschützt. Hier kann die Identität offengelegt werden. Das Gesetz sieht einige weitere Ausnahmen vom Schutz der Identität vor, etwa in Strafverfahren auf Verlangen der Strafverfolgungsbehörden und in weiteren Fällen, zum Beispiel dann, wenn dies im Rahmen interner Untersuchungen erforderlich ist oder auch notwendig für das Ergreifen von Folgemaßnahmen.

**Sind Hinweisgeber auf Basis des vorliegenden Entwurfs dennoch hinreichend geschützt? Oder wo ist der Schutz noch verbesserungswürdig?**

Diese Frage drängt sich in der Tat auf, weil durchaus einige Ausnahmen von der Anonymität bestehen. Manche Meldungen verlangen aber tatsächlich nach Aufhebung der Anonymität. Das war immer eine wichtige Aufgabe der Ombudsleute, die Hinweisgeber von der Notwendigkeit zu überzeugen, und dies ist nach meiner Erfahrung in allen Fällen gelungen. Dennoch wird es einen Spagat der Interessen geben. Mir sind auch Fälle bekannt, die derartige erdbebengleiche Folgen für Unternehmen auslösten, dass die Hinweisgeber, die ihre Anonymität aufgeben mussten, tatsächlich dann auf andere Art und Weise geschützt werden mussten.

**Inwiefern ist auf Basis des Gesetzes die Rechtssicherheit gewährleistet? Oder andersherum gefragt: Wo ist sie nicht gewährleistet?**

In jedem Fall wird der Hinweisgeber durch das Gesetz deutlich besser geschützt als zuvor. Das kann man schon als Zeitenwende und Umkehr betrachten. Whistleblower sind Helden und müssen geschützt werden. Das Gesetz bietet hier eine gute Grundlage. Die Rechtssicherheit ist in den Fällen nicht gewährleistet, die das Gesetz ausdrücklich ausgenommen hat, wie etwa die nationale Sicherheit oder Ähnliches. Hier arbeiten Hinweisgeber dann weiterhin rechtlich ungeschützt. Unklar ist in manchen Fällen auch, ob hier gesetzliche Vorgaben betroffen sind oder eben interne Richtlinien oder andere schützenswerte Tatsachen, die jedoch nicht unter den Schutz des Gesetzes fallen.

**Welche Schritte sollte das Risikomanagement für einen angemessenen Hinweisgeberschutz jetzt einleiten, sofern dies noch nicht geschehen ist?**

Für das Risikomanagement ist dringender Handlungsbedarf geboten. Das Risikomanagement sollte hier nicht nur alle Maßnahmen zum Schutz des Hinweisgebers einleiten und überwachen, sondern penibel darauf achten, wie mit entsprechenden Meldungen umgegangen wird, um Gesetzesverstöße möglichst zu vermeiden.

**Wie sind in diesem Zusammenhang Meldungen von Hinweisgebern zu dokumentieren?**

Nach dem Entwurf sieht § 11 vor, dass die Person, die in einer Meldestelle für die Entgegennahme von Meldungen zuständig ist, alle eingehenden Meldungen in „dauerhaft abrufbarer Weise unter Beachtung des Vertraulichkeitsgebots“ dokumentieren soll.

**Welche Konsequenzen drohen, wenn im Risikomanagement das Thema Whistleblowing vernachlässigt oder gar ganz ignoriert wird?**

Abgesehen von einem erheblichen Reputationsschaden für das Unternehmen drohen empfindliche Bußgelder. Verstöße gegen die wesentlichen Vorgaben des Hinweisgeberschutzgesetzes werden als Ordnungswidrigkeiten mit einer Geldbuße geahndet. Das gilt beispielsweise für Unternehmen, die keine interne Meldestelle einrichten, die Meldungen behindern oder die Repressalien gegen die hinweisgebende Person ergreifen – mithin kein funktionierendes Risikomanagement haben.

**Der Umgang mit Hinweisgebern ist in Deutschland bislang problematisch. Dabei können Whistleblower dazu beitragen, in Unternehmen Fehlentwicklungen aufzudecken, bevor**



© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2022 (https://zfrmdigital.de) - 20.06.2022 14:57

Lizenziert für .
Die Inhalte sind urheberrechtlich geschützt.



**schwerwiegende Schäden entstehen. Inwiefern kann das jetzt vorgestellte Gesetz zur Verbesserung des Hinweisgeberschutzes ein Umdenken bewirken?**

Die Wahrnehmung von Hinweisgebern in der Öffentlichkeit ist in der Tat nach wie vor problembehaftet. Die Wahrnehmung ist folgende: Whistleblower, das sind Menschen, die, so die wörtliche Übersetzung, „die Pfeife blasen". Sie bringen Rechtsverstöße wie Korruption, Verschwendung, Diskriminierung oder sexuellen Missbrauch ans Tageslicht – nicht aus Rache, sondern weil sie für ethische Werte einstehen. Gedankt wird ihnen nicht immer, ganz im Gegenteil. Dabei werden Whistleblower in der Öffentlichkeit auch als Helden gefeiert. Edward Snowden oder Julian Assange, Wikileaks, Doping-Skandal, Panama Papers, um nur wenige prominente Fälle zu nennen.

**Was ist mit den vielen kleinen Fällen von Hinweisgebern?**

Solche Fälle sind weniger spektakulär, aber wesentlich alltäglicher und sie können große Wirkung entfalten. Denken wir an die Aufdeckung des Gammelfleisch-Skandals oder die Berichte über erschütternde Vorgänge in Altenheimen. Hinweisgeber sind wichtig und hilfreich und das Gesetz wird zu einem Umdenken führen. Es geht ja nicht nur darum, Missstände des Unternehmens aufzudecken, sondern auch darum, Missstände aufzudecken, die dem Unternehmen oder Unternehmer bislang gar nicht bekannt waren. Nach wie vor sind es um die 50 Prozent der Schäden, die intern passieren, also nicht von außen verursacht werden. Hinweisgeberschutz ist gut gelebte Compliance. Das kommt am Ende vor allem auch dem Risikomanagement zugute. ■

## News

## Neuer Höchstwert bei Cyberstraftaten

Die Anzahl erfasster Cyberstraftaten hat im Jahr 2021 einen neuen Höchstwert erreicht. Die 146.363 erfassten Cyberdelikte bedeuten einen Anstieg um rund 12 Prozent gegenüber dem Vorjahr. Das geht aus dem Bundeslagebild Cybercrime 2021 hervor, den das Bundeskriminalamt veröffentlicht hat.[1] Die Entwicklung sei Ausdruck der fortschreitenden Verlagerung von Kriminalität in den digitalen Raum, stellt das BKA fest. Insbesondere die zunehmende Verzahnung internationaler Lieferketten und die Digitalisierung schaffe „eine Vielzahl neuer Tatgelegenheiten für Cyberkriminelle". Die Cybercrime-Schäden in Deutschland belaufen sich nach Berechnungen des Branchenverbands Bitkom auf 223,5 Milliarden Euro im Jahr 2021. Drastische Zunahmen gibt es insbesondere bei den Erpressungstrojanern Ransomware und bei DDoS-Angriffen. Bei einer frühzeitigen Erstattung einer Strafanzeige sei es den Strafverfolgungsbehörden möglich, schnelle und effektive Maßnahmen gegen kriminelle Cybergruppierungen zu treffen, teilt das BKA mit.

## Digitalisierung als strategische Chance

Die Digitalisierung hat für viele Finanzchefs hohe Priorität. Das geben 73 Prozent der weltweit 522 befragten CFOs in der PwC-Studie „The Digital CFO" an.[2] Dennoch steht die Digitalisierung des Finanzressorts in vielen Unternehmen oft noch am Anfang, stellt PwC fest. Dashboard-Tools für übersichtliches Reporting seien zwar weit verbreitet, Technologien wie Künstliche Intelligenz und Process Mining kämen hingegen kaum zum Einsatz. Die klassische Arbeit von Finanzabteilungen wie das Überwachen von Finanzkennzahlen, Zahlungen und Risiken beruht zu einem großen Teil auf klaren Regeln, die sich einfach standardisieren und kosteneffizient digitalisieren lassen, so Gori von Hirschhausen, Finance Consulting Leader Europe bei PwC Deutschland. Aus Sicht der Finanzleiter fehle es sowohl den Mitarbeitenden als auch dem Management an Know-how. Für viele CFOs gelte es nun, die eigene Rolle im Unternehmen und die der Finanzabteilung neu zu definieren. *fab*

### Anmerkungen

1 Bundeskriminalamt, BKA verzeichnet neuen Höchstwert bei Cyber-Straftaten – Bundeslagebild Cybercrime 2021 veröffentlicht, abrufbar unter https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220509_PM_CybercrimeBLB.html (Abruf: 11.5.2022).

2 PWC, The Digital CFO: die digitale Finanzfunktion strategisch nutzen, abrufbar unter https://www.pwc.de/de/im-fokus/finance-transformation/the-digital-cfo-die-digitale-finanzfunktion-strategisch-nutzen.html (Abruf: 10.5.2022).



© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2022 (https://zfrmdigital.de) - 20.06.2022 14:57