www.betriebs-berater.de

Betriebs Berater

75 Jahre

42 | 2021

Gewerbesteuerkürzung ... Datenlizenzen ... Whistleblowing ... Betriebsratsfähigkeit ... Recht ...

18.10.2021 | 76. Jg.
Seiten 2433–2496

BB-Rechtsprechungsreport zum Wettbewerbsrecht 2020/2021

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Dipl.-Kfm. Markus Brinkmann, CFE, und
Dipl.- Betriebsw. (FH), Dipl.-Wirtschaftsjurist (FSH) Alexandra Blank, CFE

Umsetzungspflichten für Unternehmen aus der EU-Whistleblowing-Richtlinie

In den letzten Jahren ist der Begriff des Whistleblowing immer weiter in den Fokus der Öffentlichkeit gerückt. Durch Hinweise von Whistleblowern, bspw. im Zusammenhang mit Wirecard oder den Panama Papers, wurden der Einfluss, die Bedeutung, aber auch die Auswirkungen, welche Whistleblowing mit sich bringen können, deutlich. Whistleblower können einen entscheidenden Beitrag für die Gesellschaft und Unternehmen zur Aufklärung von Compliance-Verstößen und somit zur Aufklärung und Prävention von Vermögens- und Reputationsschäden leisten. Der Schutz von Whistleblowern ist hierbei ein entscheidender Faktor zur Effektivitätssteigerung von Hinweisgebersystemen, insbesondere um eine ausreichende Anzahl an Hinweisen zu erzielen. Vor diesem Hintergrund hat die EU mit der Richtlinie 2019/1937 den Startschuss zu einem verbesserten Whistleblower-Schutz in den Mitgliedstaaten der EU gegeben. Bis zum 17.12.2021 hat die deutsche Bundesregierung noch Zeit, die Richtlinie in nationales Recht umzusetzen. Vor diesem Hintergrund besteht bei den Unternehmen unmittelbarer Handlungsbedarf, sich mit dem Hinweisgeberschutz zu befassen und entsprechende Maßnahmen zu implementieren. Im nachfolgenden Beitrag werden die Anforderungen an ein Hinweisgebersystem mit Blick auf die Umsetzung der EU-Richtlinie und allgemeine Best Practices vorgestellt.

I. Notwendigkeit zur Einrichtung von Hinweisgebersystemen

Whistleblower (Hinweisgeber) sind Personen, die Missstände im öffentlichen Interesse innerhalb einer Organisation aufdecken.[1] Sie leisten durch ihre Meldungen einen entscheidenden Beitrag zur Aufdeckung und Behebung von betrieblichen Missständen, sowohl zum Erhalt der Marktgerechtigkeit wie auch zum Schutz des Gemeinwohls.[2] Eine aktuelle Studie der Association of Certified Fraud Examiners (ACFE) identifizierte hierzu im Rahmen einer Untersuchung von über 2500 Wirtschaftsstraftaten in Unternehmen aus 125 Ländern mit einem Gesamtschaden von mehr als 3,6 Mrd. US-Dollar, dass 43 % der Fälle durch Hinweise aufgedeckt wurden. Hierbei konnte die Hälfte der Hinweise auf Mitarbeiter der betroffenen Unternehmen zurückgeführt werden (s. Abbildung 1).[3]

Ungeachtet etwaiger gesetzlicher Verpflichtungen ist die Einrichtung eines effektiven Hinweisgebersystems im Unternehmen unerlässlich. Hierfür gibt es auch für mittelständische Unternehmen eine Vielzahl von Gründen: Innerhalb des Unternehmens unterstützt ein solches System dabei, Missstände frühzeitig zu erkennen und diese zeitnah aufzuklären. Darüber hinaus birgt ein Hinweisgebersystem Schutz für Unternehmen und dessen Arbeitnehmer, insbesondere derer, die im Unternehmen durch Compliance-Verstöße weniger geschädigt werden. Darüber hinaus dient ein Hinweisgebersystem zur Abschreckung für potenzielle Täter und hat damit auch präventive Wirkung. Ein Hinweisgebersystem entfaltet auch extern positive Effekte. Durch frühzeitige Erkennung und interne Aufklärung können Hinweisgebersysteme dabei helfen, Reputations- und sonstige betriebswirtschaftliche Schäden zu minimieren. Gleichzeitig ist es Teil der positiven Außenwirkung des Unternehmens und kann damit ebenfalls einen Wettbewerbsvorteil darstellen. Ein funktionierendes Hinweisgebersystem gibt Arbeitnehmern die Sicherheit, geschützt intern Hinweise zu melden, und fördert die Vertrauenskultur im Unternehmen. Dadurch kann der Rückgriff auf externe Meldewege sowie die daraus entstehenden unternehmensschädlichen Auswirkungen (z. B. Reputationsschäden durch Presseberichterstattung) vermieden werden. Zusätzlich ist das Hinweisgebersystem ein wichtiger Bestandteil von Compliance-Management-Systemen; dadurch kann die Effektivität der Compliance-Management-Systeme gesteigert werden, welche im Rahmen von Prüfungen, z. B. gem. Prüfungsstandard 980 des Instituts der Wirtschaftsprüfer (IDW PS 980) sowie gem. Standard 37301 der International Organization for Standardization (ISO 37301), zertifiziert werden können. Besitzt ein Unternehmen ein solches System, kann dies exkulpierend und strafmildernd wirken.[4]

Trotz der gegenwärtigen Bedeutung und Relevanz von Whistleblowing ist der Hinweisgeberschutz in den Mitgliedstaaten der EU unterschiedlich stark vorhanden. So verfügt nur etwa ein Drittel der Mitgliedstaaten über einen Hinweisgeberschutz, und in den anderen Mit-

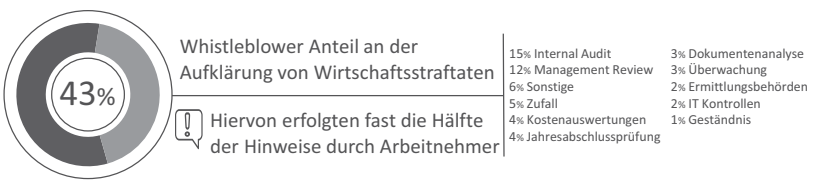

Abbildung 1: **Beitrag von Whistleblowern zur Aufklärung von Wirtschaftsstraftaten** (eigene Darstellung, Daten: ACFE, Report to the Nations, 2020, abrufbar unter https://www.acfe.com/report-to-the-nations/2020/, Abruf: 9.9.2021, S. 4 und 9)

1 Vgl. Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (WB-RL), ABlEU vom 26.11.2019, L 305, 17, ErwG 1.
2 Vgl. *Schmitt*, NZA-Beil. 3/2020, 50, 54.
3 Vgl. Association of Certified Fraud Examiners (ACFE), Report to the Nations, 2020, abrufbar unter https://www.acfe.com/report-to-the-nations/2020/ (Abruf: 9.9.2021), S. 4 und 9.
4 Vgl. Deutsches Institut für Compliance (DICO), A14 – Hinweisgeber- bzw. Whistleblowersysteme im Mittelstand, Okt. 2019, abrufbar unter https://www.dico-ev.de/wp-content/uploads/2021/03/A14_Whistleblowing_Mittelstand.pdf (Abruf: 9.9.2021), S. 3.

gliedstaaten liegt nur ein teilweiser oder sektorspezifischer Schutz vor.[5] Eine im Auftrag der Europäischen Kommission durchgeführte Studie schätzte „die potenziellen, durch einen unzureichenden Hinweisgeberschutz bedingten Ertragsausfälle allein für den Bereich des öffentlichen Auftragswesens" in der EU auf 5,8 bis 9,6 Mrd. Euro jährlich.[6] Ein wirksamer Hinweisgeberschutz ist unerlässlich, um die Meldebereitschaft der Arbeitnehmer sicherzustellen und die bereits erwähnten Vorteile frühzeitiger Meldungen zu realisieren.

II. Bisheriger Schutz von Whistleblowern in Deutschland

Im deutschen Recht gibt es bisher keinen allgemein geltenden Hinweisgeberschutz. Vielmehr existieren lediglich bereichsspezifische Normen mit Whistleblowing-Bezug, z. B. im Wertpapierhandelsgesetz und Arbeitsschutzgesetz, die Beschwerdeführer in spezifischen Fällen von ihrer Verantwortlichkeit befreien und vor Benachteiligungen schützen.[7] Grundsätzlich bedürfen Arbeitnehmer der Rechtssicherheit, um die Meldebereitschaft zu erhöhen. Seit 2008 wurden durch verschiedene Bundesministerien sechs Gesetzentwürfe zum Hinweisgeberschutz erarbeitetet, welche bisher jedoch ergebnislos blieben.[8] Mit Umsetzung der Richtlinie (EU) 2019/1937 hat die Bundesregierung die Möglichkeit, den bisher kaum vorhandenen Hinweisgeberschutz in Deutschland gesetzlich zu verankern und entsprechend den aktuellen Erfordernissen und im Einklang mit der europäischen Richtlinie ein wirksames Whistleblowing-Gesetz auf den Weg zu bringen.

III. EU-Whistleblowing-Richtlinie

1. Anwendungsbereich der EU-Whistleblowing-Richtlinie

Die Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23.10.2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (Whistleblowing-Richtlinie – WB-RL),[9] zielt auf die Etablierung eines Mindestschutzes für Hinweisgeber und auf eine Förderung des Whistleblowing ab. Grundsätzlich soll die WB-RL Hinweisgeber, deren Verwandte sowie Dritte, die mit dem Hinweisgeber in Kontakt stehen, vor Vergeltungsmaßnahmen bei Meldungen über unionsrechtliche Verstöße schützen und Unternehmen wie auch Behörden gleichermaßen zur Implementierung eines Hinweisgebersystems verpflichten. Die Richtlinie definiert verschiedene Rechtsbereiche der EU, zu denen Meldungen über unionsrechtliche Verstöße in den sachlichen Anwendungsbereich der WB-RL fallen, welche im Rahmen der Umsetzung um nationales Recht erweiterbar sind. Hierunter fallen u. a. Meldungen über Verstöße aus dem öffentlichen Auftragswesen, Finanzdienstleistungen, Produktsicherheit, Umweltschutz, öffentliche Gesundheit, Verbraucherschutz, Datenschutz sowie Rechtsakte zur Verhinderung von Geldwäsche und Terrorismusfinanzierung (Art. 2 WB-RL). Der weit gefasste persönliche Anwendungsbereich umfasst alle Hinweisgeber, die „im weitesten Sinne in einer arbeitsbezogenen Verbindung mit einem Unternehmen stehen"[10]. Dabei ist irrelevant, welche Motive den Whistleblower zur Meldung veranlasst haben. Damit jedoch ein Whistleblower durch die Richtlinie geschützt wird, muss die gemeldete Information in den Anwendungsbereich der Richtlinie fallen und dieser zum Zeitpunkt der Meldung hinreichend Grund zur Annahme haben, dass die gemeldeten Informationen wahrheitsgemäß sind und die Informationen unter Einhaltung der verfahrensrechtlichen Vorgaben offengelegt wurden. Zudem muss die gemeldete Information in den Anwendungsbereich der Richtlinie fallen (Art. 6 WB-RL).

2. Geltungsbereich des Hinweisgeberschutz

Sind die oben genannten Voraussetzungen erfüllt, so ist ein Hinweisgeber vor Repressalien und deren Androhung geschützt. Dies beinhaltet jede direkte oder indirekte Handlung im beruflichen Kontext, welche durch die Offenlegung des Hinweisgebers ausgelöst wurde und für diesen einen ungerechtfertigten Nachteil zur Folge hat. Um Hinweisgeber vor Repressalien zu schützen, beinhaltet die WB-RL Schutzmaßnahmen wie eine Beweislastumkehr. Demnach muss das betreffende Unternehmen nachweisen, dass die Benachteiligung eines Hinweisgebers aus legitimen Gründen erfolgte und nicht im Zusammenhang mit der Hinweisgabe steht (Art. 21 Abs. 5 WB-RL). Darüber hinaus erhält der Hinweisgeber Zugang zu unterstützenden Maßnahmen, wie bspw. Beratung und Prozesskostenhilfe, sowie psychologische Betreuung oder Unterstützung von zuständigen Behörden (Art. 20 WB-RL). Des Weiteren sollen Mitgliedstaaten auch „wirksame, angemessene und abschreckende Sanktionen" für natürliche und juristische Personen festsetzen, welche greifen, wenn Meldungen behindert, Repressalien gegen Hinweisgeber ergriffen werden oder die Identität des Hinweisgebers veröffentlicht werden. Gleichwohl sollen auch Sanktionen für Hinweisgeber festgelegt werden, wenn diese vorsätzlich falsche Informationen gemeldet haben (Art. 23 WB-RL).

3. Meldekanäle für Hinweisgeber

Neben den oben ausgeführten Regelungen zum Schutz von Hinweisgebern liegt ein weiterer Schwerpunkt der Richtlinie auf der Einführung interner und externer Meldekanäle, damit Verstöße anonym und vertraulich gemeldet werden können. Hierbei beschreibt eine interne Meldung die mündliche oder schriftliche Mitteilung von Informationen über Verstöße innerhalb eines Unternehmens, während externe Meldungen eine Mitteilung an eine zuständige Behörde darstellen. Die für die Entgegennahme von Meldungen zuständigen Behörden werden durch die Mitgliedstaaten bestimmt und mit angemessenen Ressourcen ausgestattet. Interne Meldekanäle sind hingegen von den Unternehmen selbst errichtet, jedoch müssen diese nicht vom Unternehmen selbst betrieben werden, sondern es besteht auch die Möglichkeit, diese an Dienstleister, wie z. B. Rechtsanwälte, Wirtschaftsprüfer etc., auszulagern. Hierbei besteht bei Unternehmen ab 50 Arbeitnehmern eine gesetzliche Pflicht zur Einrichtung interner Meldekanäle und verbundener Prozesse für Folgemaßnahmen (Art. 8 WB-RL). Ob eine gesetzliche Pflicht auch für Unternehmen mit weniger als 50 Arbeitnehmern bestehen wird, obliegt den Mitgliedstaaten bei deren Umsetzung der WB-RL. Grundsätzlich ist die Einrichtung interner Meldekanäle unabhängig von der Arbeitnehmeranzahl für jedes Unternehmen zu empfehlen.

5 Vgl. Europäisches Parlament, Whistleblower: Neue Vorschriften für EU-weiten Schutz von Informanten, 16.4.2019, abrufbar unter https://www.europarl.europa.eu/news/de/press-room/20190410IPR37529/whistleblower-neue-vorschriften-fur-eu-weiten-schutz-von-informanten (Abruf: 9.9.2021).
6 Vgl. Europäisches Parlament, Whistleblower: Neue Vorschriften für EU-weiten Schutz von Informanten, 16.4.2019, abrufbar unter https://www.europarl.europa.eu/news/de/press-room/20190410IPR37529/whistleblower-neue-vorschriften-fur-eu-weiten-schutz-von-informanten (Abruf: 9.9.2021).
7 Vgl. *Dzida/Granetzny*, NZA 2020, 1201, 1202.
8 Vgl. *Mayer*, Deutscher Anwalt Spiegel 9/2021, 3.
9 Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, ABlEU vom 26.11.2019, L 305, 17.
10 Vgl. *Dzida/Granetzny*, NZA 2020, 1201, 1202.

Interne und externe Meldewege sollten gleichrangig sein, wobei interne Meldewege bevorzugt werden, soweit mit einer internen Meldung ohne Befürchtung von Repressalien wirksam gegen einen Verstoß vorgegangen werden kann. Es besteht jedoch keine Pflicht zur vorherigen Nutzung der internen Meldekanäle. Als dritte Stufe kann zudem die Meldung eines Hinweisgebers an die Öffentlichkeit gesehen werden. Diese Offenlegung gem. Art. 15 WB-RL ist jedoch nur als ultima ratio zu verstehen, sofern der Hinweisgeber den Verstoß vorher unerfolgreich intern oder extern gemeldet hat und innerhalb der gesetzten Fristen keine geeigneten Maßnahmen ergriffen wurden. Sowohl interne als auch externe Meldungen müssen innerhalb von sieben Tagen nach Eingang bestätigt werden. Eine Rückmeldung an dem Hinweisgeber muss bei internen Meldungen innerhalb von drei Monaten und bei externen Meldungen innerhalb von sechs Monaten erfolgen. Eine mit dem Sachverhalt verbundene interne Untersuchung ist nicht an diese Fristvorgaben gebunden.[11]

4. Anforderung an die Mitgliedstaaten im Rahmen der Umsetzung

Im Allgemeinen belässt die Richtlinie den nationalen Gesetzgebern entsprechenden Handlungsraum, insbesondere bei der Verpflichtung zur Entgegennahme und Weiterverfolgung anonymer Meldungen. Gleichzeitig sollen Hinweisgeber wirksam und effektiv geschützt werden.[12] Mit der WB-RL hat die EU einen längst überfälligen und in jeder Hinsicht notwendigen Schutzrahmen für Whistleblower geschaffen. Wie viel Schutz die Richtlinie in den Mitgliedstaaten mit sich bringen wird, hängt jedoch von der jeweiligen nationalen Umsetzung ab. In Deutschland ist das Bundesministerium für Justiz und Verbraucherschutz (BMJV) von der Regierung mit der Erstellung eines Referentenentwurfs für ein Hinweisgeberschutzgesetz beauftragt worden. Zum jetzigen Zeitpunkt liegt lediglich ein nicht veröffentlichter Entwurf vom Dezember 2020 vor, welcher im Bundeskabinett diskutiert werden sollte, sich aber weiterhin in der regierungsinternen Abstimmung befindet.[13] Hauptstreitpunkt ist bisher die Erweiterung des Anwendungsbereichs der Richtlinienregelungen auf nationales Recht. Eine solche Erweiterung ist mit Blick auf einen fundierten Hinweisgeberschutz unerlässlich. Spätestens mit Verstreichen der Umsetzungsfrist bis zum 17.12.2021 können sich Hinweisgeber nach gängiger Rechtsmeinung direkt auf die Richtlinie berufen, soweit noch kein nationales Umsetzungsgesetz beschlossen wurde.[14]

IV. Implementierung eines Hinweisgebersystems

1. Interne und externe Meldewege

In Zukunft muss die Implementierung eines Hinweisgebersystems im Einklang mit dem Hinweisgeberschutzgesetz stehen; da dieses jedoch noch nicht verabschiedet wurde, können die Grundsätze der EU-Hinweisgeberrichtlinie bereits jetzt als Grundlage für die Implementierung von Hinweisgebersystemen herangezogen werden. Möglicherweise können geringfügige Anpassungen an nationales Recht später vorgenommen werden. Es sollte den Hinweisgebern die Möglichkeit eingeräumt werden, Meldungen auf unterschiedliche Art und Weise abgeben zu können, da es diesbezüglich unterschiedliche Präferenzen gibt, z. B. können Meldungen schriftlich oder telefonisch abgegeben werden. Zudem ist sicherzustellen, dass keine unbefugten Personen Zugriff auf dieses System haben, um die Vertraulichkeit und Anonymität des Hinweisgebers jederzeit sicherzustellen. Darüber hinaus sind auch Regelungen an die Form und Frist einer Eingangsbestätigung (innerhalb von sieben Tagen) wie auch Rückmeldung an den Hinweisgeber zum vorgebrachten Hinweis (innerhalb von drei Monaten) festzulegen. Welche Meldekanäle für ein Hinweisgebersystem genutzt werden sollen, ist unternehmens- und organisationsabhängig. Grundsätzlich besteht die Möglichkeit, auf ein internes und externes Hinweisgebersystem zurückzugreifen.

Bei internen Hinweisgebersystemen werden Hinweise an eine unternehmensinterne Stelle oder an einen beauftragten externen Dienstleister gemeldet. Zur Wahrung der Anonymität und Vertraulichkeit sollte es sich um einen begrenzten Personenkreis handeln, der Zugang hat bzw. in den Sachverhalt involviert wird. In Frage kommt bspw. die Rechtsabteilung, der Compliance-Beauftragte oder die Interne Revision. Bei den externen Dienstleistern kann es sich um Rechtsanwälte und Wirtschaftsprüfer handeln, da diese besonderen berufsrechtlichen Pflichten unterliegen. Der Vertrag zwischen dem Unternehmen und dem externen Dienstleister muss den besonderen rechtlichen Anforderungen an ein Hinweisgebersystem Rechnung tragen. Die Vor- und Nachteile eines intern betriebenen Systems und eines ausgelagerten Systems sind individuell abzuwägen und an den unternehmens- bzw. organisationsspezifischen Anforderungen auszurichten. Ein internes Hinweisgebersystem verursacht zunächst nur einen geringen Aufwand bei der Einführung und keine Kosten für eine externe Meldestelle. Zudem gelangen die Informationen von Hinweisgebern auf direktem Weg an die zuständige unternehmensinterne Stelle, welche in der Regel vertrauter mit den Prozessen des Unternehmens ist als unabhängige Externe. Zu berücksichtigen ist jedoch das Vertrauensverhältnis der Arbeitnehmer zu der verantwortlichen internen Stelle; mancher Hinweisgeber bevorzugt eine externe unabhängige Vertrauensperson, da diese über eine größere Distanz zum Unternehmen verfügt. Darüber hinaus verfügen extern ausgelagerte Meldestellen über ein hohes Maß an Vertrauenswürdigkeit, u. a. aufgrund vorhandener Verschwiegenheitspflichten. Außerdem ermöglicht deren fachliche Expertise zudem eine zügige Einschätzung der vorgebrachten Vorwürfe.[15] Diese fachliche Expertise kann z. B. das Wissen über Schemata von Wirtschaftskriminalität, rechtliche Kenntnisse, Interviewtechniken etc. umfassen. Im Übrigen können Unternehmen Hinweisgebern die Möglichkeit einräumen, unternehmensinterne Meldekanäle oder interne Meldekanäle, die von externen Dienstleistern betrieben werden, abzusprechen (hybrides System).

Eine Studie der EQS Group aus dem Jahr 2019 ergab, dass Unternehmen durchschnittlich drei interne Meldekanäle anbieten.[16] Vorrangiges Ziel sollte hierbei sein, dass potenzielle Verstöße unverzüglich identifiziert werden und eine Meldung an Dritte, wie Behörden oder die Öffentlichkeit, nach Möglichkeit nicht erfolgt. Idealerweise sollte ein Hinweisgebersystem einen Meldekanal auch auf Basis einer internetbasierten Kommunikationsplattform mit einem anonymisierten Dialog beinhalten. Diese Form ist aufgrund ihrer Zeit- und Ortsunabhängigkeit sowie gesicherter und anonymer Hinweisübermittlung besonders vorteilhaft. Darüber hinaus kann hierüber ebenfalls eine anforderungsgerechte Dokumentation sichergestellt werden.

11 Vgl. *Dzida/Granetzny*, NZA 2020, 1201, 1203.
12 Vgl. *Schmolke*, NZG 2020, 12.
13 Vgl. *Mayer*, Deutscher Anwalt Spiegel 9/2021, 3.
14 Vgl. *Dzida/Granetzny*, NZA 2020, 1201, 1204.
15 Vgl. DICO, A14 – Hinweisgeber- bzw. Whistleblowersysteme im Mittelstand, Okt. 2019, abrufbar unter https://www.dico-ev.de/wp-content/uploads/2021/03/A14_Whistleblowing_Mittelstand.pdf (Abruf: 9.9.2021), S. 4.
16 Vgl. EQS Group, Whistleblowing Report 2019, abrufbar unter https://whistleblowingreport.eqs.com/ (Abruf: 9.9.2021), S. 8.

Bis 2018 waren Hotlines mit 42 % der am häufigsten genutzte Meldekanal in Unternehmen. Seitdem kann eine Änderung dieses Trends verzeichnet werden. Demnach fiel die Nutzung von Hotlines im Jahr 2020 auf 33 %, womit dieser Meldeweg mit Meldungen per E-Mail und internetbasierten Hinweissystemen, welche in den letzten Jahren einen starken Anstieg verzeichneten, gleich häufig genutzt wurden.[17] Sehr effektiv ist jedoch auch die Möglichkeit, einen externen Dienstleister (z. B. Ombudsmann) über eine eigens dafür vorgesehene Telefonnummer direkt persönlich zu erreichen. Dadurch kann zwischen dem Hinweisgeber und dem Ombudsmann ein sehr effektiver Austausch stattfinden. Im Gegensatz zu Hotlines kann der Ombudsmann als ausgewiesener Experte unmittelbar ein qualifiziertes Gespräch führen und die Validität der Hinweise in der Regel gut einschätzen. Da die Präferenzen der Hinweisgeber unterschiedlich sind, ist es empfehlenswert, sowohl internetbasierte Kommunikationsplattformen (intern oder über externe Dienstleister) als auch telefonische Meldewege (über Ombudspersonen) zu betreiben. Die internetbasierten Kommunikationsplattformen erweisen sich oftmals zur Erreichung der Hinweisgeber im Ausland als vorteilhaft, vor allem wenn unterschiedliche Zeitzonen eine Rolle spielen; außerdem können verschiedene Sprachräume adressiert werden. Weitere Vorteile liegen in der sicheren Übermittlung von Daten wie auch in der Berücksichtigung von relevanten datenschutzrechtlichen Anforderungen.

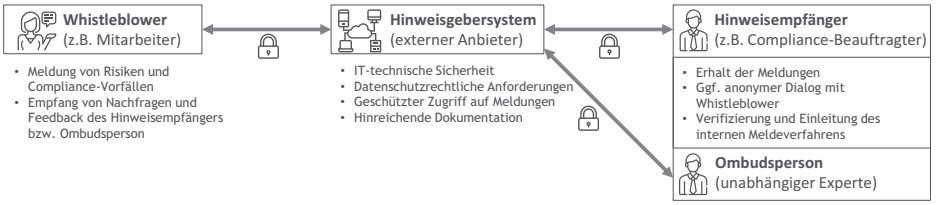

Abbildung 2: **Digitales Hinweisgebersystem mit einer eingesetzten Ombudsperson** (Quelle: eigene Darstellung)

2. Verwendung eines digitalen Hinweisgebersystems

Bei der Verwendung eines digitalen Hinweisgebersystems kann man sich mit Standardtexten behelfen, welche jedoch individuell angepasst werden müssen, um sicherzustellen, dass alle relevanten Fragen adressiert und abgefragt werden können. Zudem sind Meldekategorien zu definieren, welche einer ersten Zuordnung bzw. Themenkategorisierung dienen. Hierunter können bspw. die nachfolgenden Kategorien gefasst werden: Datenschutzverstöße, Diskriminierung, Diebstahl, Umwelt- und Gesundheitsschutz, Compliance-Verstoß, Korruption und Bestechung. Natürlich sollte auch eine allgemeine Kategorie wie „Sonstiges" vorhanden sein, in der individuelle Angaben und Detailbeschreibungen zum Sachverhalt aufgenommen werden können. Bevor ein digitales Meldesystem „live" in Betrieb genommen wird, sollte es umfangreich auf Funktionsfähigkeit getestet werden. Darüber hinaus kommen auch der Kommunikation und der Bekanntmachung eines Hinweisgebersystems eine fundamentale Bedeutung zu. Ohne klare Botschaft über Funktionsfähigkeit, Ziel und Bedeutung wird der Erfolg eines Hinweisgebersystems ausbleiben. Veröffentlichungen an allen relevanten Stellen, bspw. im Intranet, auf der Unternehmenswebseite, auf Aushängen, im Rahmen von Trainings etc. sowie in Verbindung mit Hausmitteilungen durch die Unternehmensführung („Tone from the top") tragen maßgeblich zur Akzeptanz und Wirksamkeit von Hinweisgebersystemen bei. Darüber hinaus sollten gezielte Trainings- und Schulungsmaßnahmen durchgeführt werden, um wesentliche Inhalte zielorientiert zu vermitteln und die Mitarbeiter hin zu einer „Speak-Up Kultur" zu sensibilisieren. Die Konzeption und Implementierung eines Hinweisgebersystems (telefonisch und/oder digital) sollte zur Steigerung der Effektivität und Sicherheit des Verfahrens entsprechend von externen Experten unterstützt und begleitet werden (s. Abbildung 2).

Letztlich obliegt es jedem Unternehmen selbst, welche Meldekanäle für dessen spezifische Organisation am effizientesten erscheinen und ausgewählt werden. Ungeachtet dessen, für welchen Aufbau des Hinweisgebersystems sich ein Unternehmen entscheidet, sollten die zur Anwendung kommenden Prozesse klar dokumentiert und kommuniziert werden. Hierbei sollten klare und transparente Teilprozesse, wie u. a. die Prozesse der Hinweisabgabe, Entgegennahme, Bewertung, Untersuchung und Berichterstattung, definiert werden. Darüber hinaus sollten die jeweiligen Zuständigkeiten klar geregelt sein und die Analyse und Bewertung von Hinweisen mindestens im Vier-Augen-Prinzip erfolgen, z. B. durch eine Ombudsperson und den Compliance-Beauftragten des Unternehmens. In jedem Fall muss jedoch sichergestellt werden, dass dem Hinweisgeber die Möglichkeit der Anonymität gegenüber dem Unternehmen eingeräumt wird. Dies kann z. B. durch die Anwendung ausgewählter internetbasierter Kommunikationsplattformen (anonymisierter Dialog) oder durch die Einbindung eines Ombudsmanns sichergestellt werden.

Neben den Meldekanälen kommt in einem Hinweisgebersystem eine Vielzahl an Teilprozessen zur Anwendung, welche im Vorfeld hinreichend zu planen und definieren sowie mit entsprechenden Verantwortlichkeiten zu verbinden sind und transparent kommuniziert werden müssen. Wichtig sind zudem die individuellen Rahmenbedingungen und Gegebenheiten, an welche die Bestandteile und Teilprozesse eines Hinweisgebersystems individuell anzupassen sind.

Hinweisabgabe Wie und über welche Meldekanäle können Hinweis abgeben werden?	**Entgegennahme** Wer nimmt die Hinweise entgegen, und wie erfolgt die Dokumentation?	**Bewertung** Wer ist für die Bewertung der Hinweise verantwortlich und nimmt eine Erstbewertung vor?
Benachrichtigung Wer wird über den Hinweis informiert und entscheidet Folgehandlungen?	**Untersuchung** Wie erfolgt die Untersuchung von glaubwürdigen Hinweisen?	**Berichterstattung** Wie erfolgt die abschließende Berichterstattung und Dokumentation?

Abbildung 3: **Mögliche Teilprozesse eines Hinweisgebersystems** (Quelle: eigene Darstellung)

Im Rahmen der Implementierung stellen eine unternehmensgerechte Einführung und Anpassung der vorgenannten Teilprozesse die Grundlage für die Wirksamkeit und Effektivität eines Hinweisgebersystems dar.

3. Mitarbeitertrainings zur Effektivitätssteigerung

Neben dem Aufbau des Hinweisgebersystems ist die Förderung der Akzeptanz und Sensibilisierung der Mitarbeiter ein weiterer entscheidender Faktor. Ziel sollte sein, eine hohe Akzeptanz für das Hinweisgebersystem zu erreichen. Dies ist in Unternehmen mit einer stark etablierten Compliance-Kultur leichter zu erlangen als in Unternehmen, in denen Compliance noch nicht den erforderlichen Stellenwert erreicht hat. Neben der Compliance-Kultur sind zudem im internationalen Umfeld kulturelle Besonderheiten sowie länder- und branchenspezifische Herausforderungen zu berücksichtigen. Um die Akzeptanz zu fördern,

17 Vgl. ACFE, Report to the Nations, 2020, abrufbar unter https://www.acfe.com/report-to-the-nations/2020/ (Abruf: 9.9.2021), S. 22.

muss ein klares Verständnis über Ziel, Inhalt und Nutzen von Hinweisgebersystemen geschaffen und an der Sensibilisierung der Mitarbeiter gearbeitet werden. Die Implementierung des Hinweisgebersystems sollte zudem an alle Arbeitnehmer des Unternehmens transparent und über geeignete Kommunikationswege vermittelt werden. Damit alle Mitarbeiter den gleichen Kenntnisstand haben bzw. auch über Entwicklungen und Neuerungen informiert werden, sollte eine zielorientierte Berichterstattung erfolgen und die Thematik bspw. auch bereits im Rahmen des Onboarding von neuen Mitarbeitern berücksichtigt werden.
Das Hinweisgebersystem und die damit verbundenen Sensibilisierungsmaßnahmen müssen verdeutlichen, dass die Identität von Hinweisgebern und deren Meldung vertraulich und anonym behandelt werden. Wichtig ist, die Verbindung zwischen Compliance, Risikobewusstsein und dem Hinweisgebersystem herzustellen. Vor diesem Hintergrund müssen zielorientierte Trainings und Schulungen stattfinden, die ein Bewusstsein für compliancerelevante Themen (wie bspw. Betrug, Bestechung, Korruption, Fraud im Berufsalltag usw.) und ein Risikoverständnis vermitteln, damit das Bewusstsein für „nicht-konformes" Verhalten gestärkt und damit auch eine wirksame Nutzung von Hinweisgebersystemen ermöglich wird. Solche Trainings- und Schulungsmaßnahmen verbessern einerseits die Meldebereitschaft von Mitarbeitern und andererseits die Qualität im Rahmen der Hinweismeldung. Mitarbeiter, die eine solche Schulung erhalten haben, erkennen und melden häufiger Missstände als Arbeitnehmer ohne Schulung. Gleiches gilt für die Qualität und Verwertbarkeit der gemeldeten Sachverhalte.

Abbildung 4: **Mitarbeiter-Trainings als Multiplikator zur Meldebereitschaft**
(Quelle: eigene Darstellung; Daten: vgl. ACFE, Report to the Nations, 2020, abrufbar unter https://www.acfe.com/report-to-the-nations/2020/, Abruf: 9.9.2021, S. 21)

Letztlich ist eine zielgruppenspezifische Kommunikation zum Hinweisgebersystem gegenüber Mitarbeitern und relevanten Stakeholdern unerlässlich. Ein entscheidender Faktor stellt die bisher gelebte Compliance-Kultur im Unternehmen dar, welche einen zentralen Richtungsweiser und Antrieb für das Hinweisgebersystem darstellt. Zusammenfassend kommen der verwendeten Hinweisgebersystematik, den zum Einsatz kommenden Meldekanälen sowie den an die individuellen Anforderungen und Bedürfnisse des Unternehmens angepasste Definition und Ausgestaltung relevanter Teilprozesse maßgebliche Bedeutung für die Wirksamkeit und Effektivität eines Hinweisgebersystems zu. Zur Förderung der Akzeptanz und Sensibilisierung der Mitarbeiter sollten zielorientierte Trainings und regelmäßige Schulungsmaßnahmen herangezogen werden.

V. Ausblick zur Umsetzung der EU-Whistleblowing-Richtlinie

Durch die EU-Hinweisgeberrichtlinie und die folgende Umsetzung in Form eines nationalen Hinweisgeberschutzgesetzes sind anwendungspflichtige Unternehmen dazu verpflichtet, Whistleblowing aktiv im Unternehmen zu fördern, um Missstände aufzudecken und daraus entstehende Schäden zu begrenzen. Ggf. ergeben sich für international tätige Unternehmen auch weitere Anforderungen an Hinweisgebersystemen aus ausländischen Rechtsordnungen. Auch für Unternehmen, die bereits über ein Hinweisgebersystem verfügen, ist es nun an der Zeit, die Wirksamkeit ihres Systems zu prüfen und weiterzuentwickeln. Hinweisgebersysteme sollten hierbei grundsätzlich individuell an die Bedürfnisse des jeweiligen Unternehmens angepasst werden. Der Schutz von Whistleblowern ist dabei ein grundlegender Bestandteil zur Akzeptanz und Effektivität eines Hinweisgebersystems und integraler Bestandteil der EU-Hinweisgeberrichtlinie. Insbesondere durch den Einsatz von internetbasierten Kommunikationsplattformen mit anonymisiertem Dialog und erfahrenen Ombudspersonen kann eine angemessene Anzahl qualifizierter Hinweise sichergestellt werden, die eine gute Grundlage für die ggf. notwendige Weiterverfolgung beinhalten. Darüber hinaus kann die Compliance-Kultur im Unternehmen ein entscheidender Einflussfaktor im Hinblick auf die Akzeptanz des Hinweisgebersystems sein. Die gezielte Einbindung unternehmensinterner Stakeholder kann hierbei als geeigneter Multiplikator zur Förderung der Akzeptanz herangezogen werden.

VI. Zusammenfassung

1. Grundsätzlich ist jedes Unternehmen angehalten, sich mit dem Thema Whistleblowing auseinanderzusetzen, entsprechende Maßnahmen zu prüfen und bedarfsgerecht einzuführen oder anzupassen.
2. Unternehmer mit 50 oder mehr Arbeitnehmern sind auf Basis der EU-Hinweisgeberrichtlinie verpflichtet, ein wirksames Hinweisgebersystem zu implementieren, Whistleblower entsprechend zu schützen und die Vorgaben der WB-RL umzusetzen.
3. Whistleblower leisten einen entscheidenden Beitrag bei der Aufklärung von Missständen und der Abwendung von Schäden für das Unternehmen.
4. Der Schutz von Whistleblowern ist als ein entscheidender Beitrag zur Funktionalität eines Hinweisgebersystems anzusehen.
5. Trainings von Mitarbeitern und deren Sensibilisierung sind ein wirksamer Multiplikator für die Effektivitätssteigerung von vorhandenen Hinweisgebersystemen.
6. Zur Sicherstellung der Anonymität gegenüber dem Unternehmen sind bei telefonisch abgegebenen Hinweisen Ombudsleute am besten in der Lage, die Anforderungen zu erfüllen. Ombudspersonen können neben dem Schutz der Whistleblower mit ihrer Expertise eine qualitative Beurteilung der vorgebrachten Anschuldigungen beitragen.
7. Insbesondere digitale Hinweisgebersysteme mit anonymisiertem Dialog können zur Erfüllung der Anforderungen gemäß WB-RL maßgeblich beitragen.

Dipl.-Kfm. Markus Brinkmann, CFE, ist Partner und Fachbereichsleiter im Bereich Forensic, Risk & Compliance bei der BDO AG Wirtschaftsprüfungsgesellschaft. Er ist bei BDO Global für die Koordination von Forensic und Risk Advisory in der EMEA Region zuständig.

Dipl.-Betriebsw. (FH), Dipl.-Wirtschaftsjurist (FSH) Alexandra Blank, CFE, ist Senior Manager und Prokurist im Bereich Forensic, Risk & Compliance bei der BDO AG Wirtschaftsprüfungsgesellschaft. Sie ist internationale Expertin zum Thema Hinweisgeberschutz.