www.compliance-berater.de

Compliance Berater

5 / 2022

Betriebs-Berater Compliance

28.4.2022 | 10.Jg
Seiten 137–180

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

CB-BEITRAG

Dr. Burkhard Fassbach, RA, Dr. Frank Hülsberg, WP/StB, und Prof. Dr. Hansgeorg Spamer, RA

Hinweisgeberschutz durch Vertrauensanwälte

Am 17.12.2021 ist die EU-Whistleblower-Richtlinie (EU-WBRL) in Kraft getreten.[1] EU-Justizkommissar Didier Reynders definierte die Zielsetzung wie folgt: „Whistleblower sollen sich sicher fühlen können, um über Verstöße zu sprechen, die das öffentliche Interesse bedrohen, ohne Vergeltungsmaßnahmen für ihren Mut befürchten zu müssen."[2] Dem Enttarnungsrisiko kann am besten durch anonymes Whistleblowing begegnet werden. Der deutsche Referentenentwurf des Hinweisgeberschutzgesetzes (HinSchG-E) vom 26.11.2020 sah jedoch lediglich ein Vertraulichkeitsgebot – mit weitreichenden Ausnahmen – vor. So wären unternehmensinterne Meldestellen im Rahmen von Ermittlungs- und Gerichtsverfahren verpflichtet worden, auf Anordnung der Staatsanwaltschaft oder des Gerichts die Identität des Hinweisgebers – auch ohne dessen Einwilligung – weiterzugeben; dies entspricht der geltenden Rechtslage. In diesem Kontext zeigt der Beitrag auf, wie – unabhängig von der gesetzgeberischen Aktivität in Deutschland – eine Anonymitätssicherung durch die Einschaltung von Vertrauensanwälten gelingen kann.

I. Anonymität

Die Wahrung der Anonymität ist für den Hinweisgeberschutz elementar. „Ich kann jedem Hinweisgeber nur raten, seine Identität nicht preiszugeben", zitiert die Frankfurter Allgemeine Zeitung vom 16.10.2021 den Frankfurter Vertrauensanwalt Rainer Buchert.[3] So bietet auch das Bundeskartellamt Hinweisgebern die Möglichkeit, anonyme Hinweise abzugeben und hat dazu ein standardisiertes Hinweisgebersystem eingerichtet, womit eine technische Rückverfolgung der Hinweise unmöglich ist. Das Bundeskartellamt gibt Hinweisgebern den Ratschlag: „Bitte achten Sie darauf, dass Sie selbst keine Informationen eingeben, die Rückschlüsse auf Ihre Person zulassen."[4] Das Whistleblower-Netzwerk e. V. fordert: „Anonymitätssicherung ist nur einer von mehreren Wegen des Whistleblowerschutzes, oft aber angesichts des Verbreitungsgrades der Information praktisch nicht möglich. Anonymes Whistleblowing muss vom Grundrechtsschutz erfasst werden. Ein kultureller Wandel wird aber durch offenes Whistleblowing stärker gefördert."[5]

Zur dogmatischen Einordnung: Gemessen an der Modalität der Meldung ist zwischen offenem, vertraulichem und anonymem Whistleblowing zu differenzieren, also danach, ob der Hinweisgeber seine eigene Identität von vornherein offenlegt, der Adressat sie absprachegemäß nicht mit Dritten teilen soll oder der Hinweisgeber sie gegenüber sämtlichen Beteiligten planmäßig geheim hält.[6] Die EU hat den Mitgliedstaaten die Entscheidung überlassen, ob juristische Personen des privaten und öffentlichen Sektors und zuständige Behörden verpflichtet sind, anonyme Meldungen von Verstößen entgegenzunehmen und Folgemaßnahmen zu ergreifen.[7] Der Referentenentwurf des Hinweisgeberschutzgesetzes (HinSchG-E) vom 26.11.2020 sah lediglich ein Vertraulichkeitsgebot vor.[8] Die Meldestellen haben die Vertraulichkeit der Identität der hinweisgebenden Person zu wahren. Die Identität darf ausschließlich den Personen, die für die Entgegennahme von Meldungen oder für das Ergreifen von Folgemaßnahmen zuständig sind, bekannt werden, § 8 HinSchG-E. Der HinSchG-E sah keine verpflichtende Nachverfolgung anonymer Meldungen vor. Begründet wurde dies wie folgt: Um das neue Hinweisgeberschutzsystem nicht zu überlasten und erste Erfahrungen sowohl interner wie auch externer Meldestellen abzuwarten, ist keine Pflicht zur Bearbeitung anonymer Hinweise vorgesehen. Denn damit einhergehen würden nicht nur zusätzliche Kosten für die notwendigen technischen Vorrichtungen, sondern auch die Gefahr von denunzierenden Meldungen und einer Überlastung der Meldestellen.[9]

1 Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019, hier abrufbar: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L1937&from=EN; vgl. grundlegend: *Colneric/Gerdemann*, Die Umsetzung der Whistleblower Richtlinie in deutsches Recht, HSI-Schriftenreihe Band 34, Frankfurt am Main 2020.

2 Vgl. Pressemitteilung der Europäischen Kommission vom 17.12.2021, hier abrufbar: https://germany.representation.ec.europa.eu/news/neue-vorschriften-zum-schutz-von-whistleblowern-treten-heute-kraft-2021-12-17_de.

3 Vgl. *Jung*, FAZ v. 16.10.2021, 28.

4 Abgerufen unter https://www.bundeskartellamt.de/DE/Kartellverbot/Anonyme_Hinweise/anonymehinweise_artikel.html am 28.2.2022.

5 Vgl. These 9 der „10 Thesen zu Whistleblowing" des Whistleblower Netzwerk e. V., abgerufen unter https://www.whistleblower-net.de/pdf/10Thesen_10Elemente_WBNW.pdf am 28.2.2022.

6 Vgl. *Gerdemann*, RdA 2019, 16, 17.

7 Vgl. Erwägungsgrund 34 EU-WBRL.

8 HinSchG-E vom 26.11.2020, hier abrufbar: https://www.whistleblower-net.de/wp-content/uploads/2021/02/2020_11_26-Referentenentwurf-Whistleblowing-BMJV-1.pdf.

9 Vgl. Begründung zum HinSchG-E, S. 31.

Diese Begründung des Referentenentwurfs war im Schrifttum scharfer Kritik ausgesetzt. Überzeugend sind die Ausführungen von *Johannes Dilling*.[10] Whistleblowing kann nur dann effektiv sein, wenn auch anonyme Meldungen zugelassen werden. Aus der Legalitätspflicht folgt, dass Unternehmen auch anonymen Hinweisen, welche auf rechtliches Fehlverhalten hindeuten, nachgehen müssen.[11] Ob potentielle Hinweisgeber ohne die Implementierung anonymer Meldewege überhaupt bereit sein werden, Informationen weiterzugeben, wird entscheidend von der rechtlichen Ausgestaltung und praktischen Einhaltung des Vertraulichkeitsschutzes abhängen. Jedenfalls sollte es eine zwingende Pflicht zur Weiterverfolgung anonymer Meldungen geben. Es ist kein Grund erkennbar, warum eine anonyme Meldung nicht mit der gleichen Sorgfalt weiterverfolgt werden sollte wie eine vertrauliche oder offene Meldung, insbesondere wenn sie belastbare Information zu gravierenden Compliance-Verstößen enthält. In Deutschland entscheiden sich über die Hälfte der Hinweisgeber für eine anonyme Erstmeldung.[12] Das Vertrauen in ein Hinweisgebersystem ist nur durch die glaubhafte Gewährung einer umfassenden Anonymität zu erreichen.[13] Auch die Gefahr von denunzierenden Meldungen und einer Überlastung der Meldestellen kann durch wissenschaftliche Studien nicht belegt werden.[14]

Missbräuchliche Meldungen, die lediglich opportunistischer Natur sind und dazu dienen, jemanden gezielt anzuschwärzen, sind ein seltenes Phänomen. So wurden bei einer Schweizer Studie lediglich 3 Prozent der Meldungen als missbräuchlich eingestuft.[15] Hinweisgeber sollen nach Art. 6 Abs. 1 EU-WBRL nur dann geschützt sein, wenn sie zum Zeitpunkt der Meldung angesichts der Umstände und der verfügbaren Informationen hinreichenden Grund zu der Annahme haben, dass die von ihnen gemeldeten Sachverhalte der Wahrheit entsprechen. Diese Anforderung ist eine wichtige Schutzvorkehrung gegen böswillige oder missbräuchliche Meldungen, da sie gewährleistet, dass Personen keinen Schutz erhalten, wenn sie zum Zeitpunkt der Meldung willentlich und wissentlich falsche oder irreführende Informationen gemeldet haben. Gleichzeitig wird mit dieser Anforderung gewährleistet, dass der Schutz auch dann gilt, wenn ein Hinweisgeber in gutem Glauben ungenaue Informationen über Verstöße gemeldet hat.[16] Für die betroffenen Personen gelten nach Art. 22 EU-WBRL die Wahrung der Unschuldsvermutung, die Verteidigungsrechte sowie das Recht auf Anhörung.

Grundsätzlich müssen sich Mitarbeiter mit Hinweisen zunächst an die vom Unternehmen vorgesehenen Ansprechpartner (etwa die Leitung des Compliancebereichs oder eine externe Ombudsperson) wenden. Eine interne Klärung kann dann unzumutbar sein, wenn die Geschäftsleitung an Straftaten beteiligt ist, diese duldet oder wenn es sich um besonders schwerwiegende Straftaten handelt. Die Hinweisgebersysteme sind nur wirksam, wenn Hinweisgeber effektiv geschützt sind und Vertrauen in die Folgemaßnahmen haben. Steht der Vorstand im Verdacht, in Compliance-Verstöße involviert zu sein, kann ein direkter Kanal zum Aufsichtsrat die Meldebereitschaft potentieller Hinweisgeber steigern und im Unternehmensinteresse liegen.[17]

Nach Art. 10 EU-WBRL soll der Hinweisgeber in Zukunft auch bei direkter externer Meldung an die Behörden Schutz genießen. Im Wettbewerb mit den Hinweisgebersystemen der Behörden können die unternehmensinternen Meldekanäle nur dann bestehen, wenn sie ebenfalls anonyme Meldungen ermöglichen. Solche anonymen Systeme sind bei den Landeskriminalämtern, dem Bundeskartellamt und der BaFin schon heute im Einsatz. Zur Klarstellung: Die Einrichtung anonymer Meldekanäle wäre den Unternehmen nach dem HinSchG-E nicht verboten worden, sie wäre lediglich nicht verpflichtend gewesen. Der HinSchG-E sah ausdrücklich vor, dass anonyme Hinweisgeber unter die Schutzbestimmungen fallen, wenn ihre zunächst verdeckte Identität bekannt wird, § 27 Abs. 1 Satz 2 HinSchG-E. Die Frage der Einrichtung eines vertraulichen oder anonymen Whistleblowing-Systems war demnach eine Ermessensentscheidung (Business Judgment).

Anonyme Meldekanäle gelten in der herrschenden Compliance-Literatur als „Best Practice". International tätige Unternehmen sollten sich auch an den Richtlinien des US-Justizministeriums (DOJ) zur Evaluierung von Compliance-Programmen orientieren.[18] Es steht zu erwarten, dass das DOJ – nach Siemens, Bilfinger und VW – auch in Zukunft deutsche Unternehmen unter die Aufsicht eines Compliance Monitor stellen wird. Die amerikanischen Strafverfolgungsbehörden fragen in Bezug auf die Beurteilung der Effizienz der Hinweisgebersysteme ganz konkret danach, ob anonyme Meldungen ermöglicht werden: „Effectiveness of the Reporting Mechanism – Does the company have an anonymous reporting mechanism and, if not, why not?"[19] Grundsätzlich beurteilt das DOJ somit nur anonyme Meldekanäle als effizient.

II. Ausnahmen vom Vertraulichkeitsgebot

Für den Schutz der Identität des Hinweisgebers wären die Regelungen in § 9 HinSchG-E über die Ausnahmen vom Vertraulichkeitsgebot zu beachten gewesen. Die Vorschrift diente der Umsetzung von Art. 16 Abs. 2 der EU-WBRL, wonach die Identität des Hinweisgebers sowie alle anderen Informationen, aus denen die Identität des Hinweisgebers direkt oder indirekt abgeleitet werden kann, nur offengelegt werden dürfen, wenn dies nach Unionsrecht oder nationalem Recht eine notwendige und verhältnismäßige Pflicht im Rahmen der Untersuchungen durch nationale Behörden oder von Gerichtsverfahren darstellt, so auch im Hinblick auf die Wahrung der Verteidigungsrechte der betroffenen Person.

Die EU-WBRL verlangt eine Abwägungsentscheidung im Hinblick auf die Weitergabe der Identität der hinweisgebenden Person, deren Notwendigkeit dem Verhältnismäßigkeitsgrundsatz folgt. Abzuwägen ist zwischen dem berechtigten Interesse der meldenden Person an der vertraulichen Behandlung ihrer Identität auf der einen und dem Interesse der Strafverfolgungs- und Verwaltungsbehörden an der Aufklärung eines Sachverhaltes und der Verfolgung von Straftaten auf der anderen Seite. In der Regel hat das Interesse der hinweisgebenden Person an der Vertraulichkeit ihrer Identität ein großes Gewicht und kann daher nur in begründeten Fällen ohne die Zustimmung dieser Person hinter die Interessen an einer Weitergabe zurück-

10 Vgl. *Dilling*, CCZ 2021, 60 ff.
11 Vgl. *Dilling* CCZ 2021, 63.
12 Vgl. *Colneric/Gerdemann* (Fn. 1), S. 135 ff.
13 Vgl. Ernst & Young, Excisting Practice in Compliance: Stand und Trends zum Integritäts- und Compliance-Management in Deutschland, Österreich und Schweiz, 2016.
14 Vgl. Whistleblowing Report 2021 der Fachhochschule Graubünden.
15 Vgl. Studie der HTW Chur „Whistleblowing Report 2018".
16 Vgl. *Colneric/Gerdemann* (Fn. 1), S. 178.
17 Vgl. *Fassbach/Hülsberg*, BOARD – Zeitschrift für Aufsichtsräte, 2022, 28 ff.
18 Vgl. U. S. Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs (Updated June 2020), hier abrufbar: https://www.justice.gov/criminal-fraud/page/file/937501/download.
19 Vgl. U. S. Department of Justice Criminal Division (Fn. 18), S. 6.

treten. Sinn und Zweck der Meldestellen für hinweisgebende Personen ist es gerade, dass diese im Vertrauen auf den Schutz ihrer Identität eine Meldung machen können und durch die vertrauliche Behandlung vor Repressalien geschützt werden.
Mit § 4 Abs. 3 HinSchG-E hätte der Gesetzgeber die aktuelle Rechtslage nicht geändert, wo nach Anwendung des Strafprozessrechts die Weitergabe der Identität im Rahmen von Ermittlungs-, Verwaltungs- oder Gerichtsverfahren generell möglich ist – allerdings auch erforderlich sein muss. Zuständig für diese Abwägungsentscheidung ist allein die jeweils die Herausgabe der Identität anordnende Stelle entsprechend der für sie geltenden gesetzlichen Vorgaben, also im Falle strafrechtlicher Ermittlungen die Staatsanwaltschaft und das Gericht.
Im Ergebnis bedeutet dies, dass die Identität von Hinweispersonen faktisch nur dann geschützt ist, wenn keine organisationsinterne Stelle Kenntnis von der Identität hat. Ermittlungsbehörden und Gerichte entscheiden autonom nach ihrer Aufgabenzuweisung und den für sie geltenden Verfahrensregelungen, ob sie sich Kenntnis von der Identität einer Hinweisperson verschaffen wollen. Deshalb können unternehmensinterne Funktionen oder Funktionsträger Hinweispersonen die Vertraulichkeit ihrer Identität nicht zusagen. Die EU-WBRL enthält nicht nur in den Erwägungsgründen, sondern unmittelbar in der Richtlinie Schranken für die Offenlegung der Identität von Hinweispersonen (Art. 16 Abs. 2 und 3): „notwendig und verhältnismäßig". Der HinSchG-E enthielt keine Schranken, sondern öffnete nur das Vertraulichkeitsgebot: „[…] dürfen weitergegeben werden in Strafverfahren auf Verlangen der Strafverfolgungsbehörden". Hinsichtlich des „Müssens" wird auf das Strafprozessrecht verwiesen mit der Klarstellung in der Begründung, dass der Meldestelle insoweit kein Ermessenspielraum zusteht. Mittel der Strafverfolgungsbehörden sind Auskunftsersuchen, zeugenschaftliche Vernehmung und Durchsuchung.[20]

III. Anonymitätssicherung durch Vertrauensanwälte

Wenn unternehmensinterne Meldestellen den Schutz der Identität des Hinweisgebers nicht zusagen können, bietet sich der Hinweisgeberschutz durch Vertrauensanwälte an. In der Begründung zu § 14 HinSchG-E (Organisationsformen interner Meldestellen) wurde nochmals ausdrücklich klargestellt, dass externe Anwälte als Ombudspersonen mit der Einrichtung und dem Betreiben der internen Meldestelle beauftragt werden können. Die Vereinigung deutscher Vertrauensanwälte e. V. definiert das Konzept des externen Vertrauensanwalts wie folgt: „Ombudspersonen werden von Unternehmen bestellt, um Hinweise über potenzielle Straftaten im Unternehmen zu erlangen. Hinweisgeber können auf diesem Weg Informationen in einem geordneten Verfahren übermitteln, ohne dabei ihre Identität preisgeben zu müssen. Wenn und soweit gewünscht, wahrt der Vertrauensanwalt ihre Anonymität gegenüber dem Unternehmen. Hemmschwellen bei Hinweisgebern werden durch die Zusicherung von Vertraulichkeit überwunden. Das Unternehmen wiederum erhält verlässliche Informationen, auf deren Grundlage über die weiteren Schritte (Aufklärung, Beseitigung, arbeitsrechtliche Maßnahmen, Strafverfolgung) entschieden werden kann."[21]
Für den Hinweisgeberschutz sind (1) die anwaltliche Verschwiegenheitspflicht des Vertrauensanwalts und (2) spezifische Regelungen im Mandatsvertrag mit dem Unternehmen von zentraler Bedeutung. Eine typische Regelung im Mandatsvertrag ist der (unwiderrufliche) Verzicht des Auftraggebers auf Auskunftsansprüche aus dem Anwaltsvertrag hinsichtlich der Identität von Hinweispersonen. Eine andere Regelung ist die Verpflichtung des Auftraggebers, den Vertrauensanwalt nur mit Zustimmung der Hinweisperson von der anwaltlichen Schweigepflicht zu entbinden. Beide Regelungen wirken nur im Verhältnis der Parteien des Mandatsvertrages.[22] So weit, so klar.
Eine in der Praxis verbreitete Klausel im Mandatsvertrag zwischen dem Vertrauensanwalt und dem Unternehmen führt jedoch oft zu einem Dilemma für den Vertrauensanwalt: „Der Vertrauensanwalt leitet sämtliche Informationen, in dem mit dem Hinweisgeber besprochenen Umfang, an die entsprechende Stelle im Unternehmen zur weiteren Bearbeitung weiter." Demnach darf der Vertrauensanwalt keine Informationen weiterleiten, die auf die Identität des Hinweisgebers schließen lassen. Filtert er aber Informationen und hält Teile zurück, kann sein Auftraggeber seiner Legalitätspflicht nicht vollständig nachkommen. Nach den Richtlinien des DOJ muss die Compliance Funktion des Unternehmens ohnehin jederzeit Zugang zu den (allen) vom Hinweisgeber gemeldeten Informationen haben, um als wirksam zu gelten: „Has the compliance function had full access to reporting and investigative information?"[23] Dieses Dilemma wird der Vertrauensanwalt nach der geltenden Rechtslage zu Lasten des Hinweisgebers lösen.
Eine Gefahr für den Schutz der Identität des Hinweisgebers ergibt sich auch aus der Rechtsprechung des Landgerichts Bochum.[24] Demnach besteht kein Beschlagnahmeschutz für Compliance-Ombudsleute. Eine Beschlagnahmefreiheit der dem Rechtsanwalt anvertrauten Unterlagen kann somit nicht zugesichert werden. Das Landgericht Bochum hat ausdrücklich eine Beschlagnahme durch die Staatsanwaltschaft beim Ombudsanwalt zum Zwecke der Erforschung der Identität eines Hinweisgebers zugelassen und dies wie folgt begründet: § 97 Abs. 1 Nr. 3 StPO schützt nur das Vertrauensverhältnis zwischen dem Zeugnisverweigerungsberechtigten und dem im konkreten Strafverfahren Beschuldigten. Zwischen dem Compliance-Ombudsmann und dem Hinweisgeber besteht mit Blick auf die Erlangung von Informationen kein schutzwürdiges mandatsähnliches Vertrauensverhältnis. Auch ein unmittelbar aus der Verfassung hergeleitetes Beschlagnahmeverbot besteht nicht, weil im Verhältnis zwischen Ombudsmann und anonymen Hinweisgebern keine besonderen Umstände vorliegen, die ein solches gebieten könnten.
Die Hoffnung, dass es sich bei der Entscheidung des Landgerichts Bochum um eine unglückliche Einzelmeinung handelte, ist nach der Jones-Day-Entscheidung des Bundesverfassungsgerichts[25] nicht mehr aufrechtzuerhalten. Das Bundesverfassungsgericht hat die wesentlichen Argumentationslinien des Landgerichts Bochum bestätigt. Es betont dabei, dass allein die Stellung des Rechtsanwalts als unabhängiges Organ der Rechtspflege nicht ausreicht, um aus der Verfassung einen in allen Fällen geltenden Beschlagnahmeschutz abzuleiten. Im Übrigen gebiete es die Verfassung, den staatlichen Ermittlungsbehörden grundsätzlich zu ermöglichen, jeden verfügba-

20 Vgl. *Frank*, Vortrag beim Ombudsleutetreffen von Transparency International Deutschland e. V. am 18.11.2021, Slide 19.
21 Vgl. German Ombudsman Association – Vereinigung deutscher Vertrauensanwälte e. V., https://german-ombudsman-association.de/vertrauensanwaelte/.
22 Vgl. *Frank* (Fn. 20), Slide 27.
23 Vgl. U. S. Department of Justice Criminal Division (Fn. 18), S. 7.
24 LG Bochum, Beschl. v. 16.3.2016 – II-6 Qs 1/16, NStZ 2016, 500 mit Praxiskommentar von Staatsanwalt *Marc Sotelsek*, Bochum.
25 Az. 2 BvR 1405/17; 2 BvR 1780/17.

ren Spuren- und Beweisansatz zu verfolgen und zu verwerten. Einschränkungen der staatlichen Pflicht zur umfassenden Sachverhaltsaufklärung bedürfen daher stets einer besonderen Rechtfertigung.[26]

Für die Praxis steht durch die Entscheidung des Bundesverfassungsgerichts – wie auch zuvor durch die Entscheidung des Landgerichts Bochum – fest, dass es sich bei der Tätigkeit des Ombudsmanns um eine anwaltliche Tätigkeit handelt. Denn es macht keinen Sinn, sich über das Verhältnis der §§ 97 StPO und 53 StPO Gedanken zu machen, wenn man die Voraussetzungen des § 53 StPO schon nicht als erfüllt ansieht. Die Frage, ob es Fälle gibt, bei denen zwar ein Zeugnisverweigerungsrecht besteht, gleichwohl aber kein Beschlagnahmeschutz, stellt sich nur dann, wenn man dem Grunde nach ein Zeugnisverweigerungsrecht anerkennt. Dies hat die Rechtsprechung als selbstverständlich bejaht.[27]

IV. Aufgaben des Vertrauensanwalts

Die Aufgaben des Vertrauensanwalts beschränken sich nicht nur auf eine Entgegennahme und Weiterleitung der Meldungen und damit auf eine Art „Zustellerfunktion". Eine zentrale Aufgabe eines Vertrauensanwalts ist, eine erste Bewertung der Meldungen vorzunehmen und der Geschäftsführung Handlungsempfehlungen zu geben. Die Geschäftsführung ist bei einem begründeten Verdacht von Gesetzes- oder sonstigen Compliance-Verstößen zur Einleitung einer internen Ermittlung berufen. Ein Ermessen hat die Geschäftsführung nicht, lediglich einen Beurteilungsspielraum, ob die Voraussetzungen vorliegen, insbesondere ob ein hinreichender Verdacht auf Compliance-Verstöße besteht. Dabei gilt: Nicht jeder Verstoß z.B. gegen eine interne Kalkulationsrichtlinie wird eine interne Untersuchung auslösen müssen. Eine solche kann dann anstehen, wenn es um den begründeten Verdacht einer aus dem Unternehmen heraus begangenen Straftat oder Ordnungswidrigkeit geht – z.B. Betrug, Bestechung, Geldwäsche oder Datenmissbrauch. Die kritische Verdachtsschwelle lässt sich nicht abstrakt definieren. Sie hängt von der Authentizität und Schlüssigkeit der Hinweise sowie der Schwere der Folgen für das Unternehmen im Falle einer Bestätigung der Verdachtsmomente ab.

In praxi haben sich hier Kriterien herausgebildet, die der Vertrauensanwalt bei seiner Handlungsempfehlung berücksichtigen muss:

- Werden Namen, Daten, Fakten zu den Beteiligten des Vorfalls angegeben? Wie aufwändig ist es, diese Hinweise zusammenzutragen?
- Wie ist die Nachvollziehbarkeit des Sachverhaltes? Werden Beweise geliefert?
- Ist der geschilderte Sachverhalt schlüssig/möglich (war die beschuldigte Person zu dem Zeitpunkt beschäftigt, hatte sie die benötigten Kompetenzen etc.)?
- Stimmen die verwendeten Fachbegriffe und die unternehmenseigene Nomenklatur?
- Beruht der Inhalt auf eigener Wahrnehmung des Hinweisgebers oder auf fremden Aussagen?
- Wurde dieser Sachverhalt bereits in der Vergangenheit behandelt?
- Meldet sich der Hinweisgeber mit Klarnamen? Bei Anonymität: Gründe für gewünschte Anonymität?
- Besteht die Bereitschaft zur Beantwortung von Rückfragen?
- Wie hoch ist das Risiko für den Hinweisgeber?
- Entsteht womöglich sogar ein wirtschaftlicher Vorteil für den Hinweisgeber oder einen Nahestehenden?

Diese Kriterien sind nicht abschließend und erfordern teilweise subjektive Einschätzungen.[28]

Ein Rechtsanwalt, der einen brisanten Hinweis an ein Unternehmen weiterleitet, hat das Unternehmen auch darüber zu informieren, wenn dem Unternehmen selbst Gefahren drohen. Hier steht die Unternehmensgeldbuße gemäß § 30 OWiG im Raum und in Zukunft das geplante Verbandssanktionengesetz. Auch dies gehört zu den Tätigkeiten einer anwaltlichen Ombudsperson.[29]

Zu den Aufgaben eines Vertrauensanwalts sollen dagegen keine Tätigkeiten gehören, die Anwälte oder Wirtschaftsprüfer im Auftrag des Unternehmens bei einer Internal Investigation übernehmen, um hier Interessenkonflikte zu vermeiden.[30] Die „Standards of Practice" der International Ombudsman Association konstatieren deutlich: „The Ombudsman does not participate in any formal investigative or adjudicative procedures. Formal investigations should be conducted by others. When a formal investigation is requested, the Ombudsman refers individuals to the appropriate offices or individual."[31] Zwar übernehmen Rechtsanwalts- und Wirtschaftsprüfungsgesellschaften im Rahmen des „Case Management" als externe Meldestelle neben der Entgegennahme der Hinweise auch die Internal Investigation als Folgemaßnahme im Auftrag des Unternehmens; sie werden dann aber nicht explizit als Vertrauensanwälte tätig.

V. Lösungsansätze für Vertrauensanwälte

Einzelne Ombudsleute versuchen, die aufgezeigte Problematik der Beschlagnahme über die Gestaltung einer „Doppelmandatierung" zu lösen. Grundlegend soll dabei der Ombudsmann-Vertrag mit dem Unternehmen sein, der ausdrücklich das Entstehen eines Mandates mit dem Hinweisgeber gestatten soll. Die Vertragsparteien gehen in dieser Konstruktion davon aus, dass aufgrund der Eigenart der Ombudsfunktion eine Doppelmandatierung möglich ist und angesichts des vorrangigen Interesses an Informationen eine Interessenkollision nicht vorliegt. In der Folge würde dann der Vertrauensanwalt auf Wunsch mit einem Hinweisgeber einen entsprechenden eigenen Vertrag schließen. Die Gestaltung der „Doppelmandatierung" ist in der Praxis aber nicht verbreitet und könnte womöglich auch als Umgehung der Rechtsprechung gewertet werden, wonach zwischen dem Hinweisgeber und dem Ombudsmann kein Mandats- oder mandatsähnliches Verhältnis besteht. Die Doppelmandatierung ist daher im Ergebnis abzulehnen. Wesentlicher Grund ist der praktisch nicht mögliche Ausschluss von Interessenkonflikten, sofern der Vertrauensanwalt „Diener zweier Herren" mit möglicherweise divergierenden Interessen ist; er muss Schutzmaßnahmen für den Hinweisgeber auf anderem Wege erreichen.

Zeugnisverweigerungsberechtigte Vertrauensanwälte sollten als Reaktion auf die Rechtsprechung des Bundesverfassungsgerichts und

26 Vgl. *Rudolph*, StraFo 2019, 57 ff.; als Exzerpt auch hier abrufbar: https://www.rudolph-recht.de/beschlagnahme-beim-compliance-rechtsanwalt-ombudsmann-nach-der-jones-day-entscheidung-des-bverfg/.

27 Vgl. *Rudolph*, StraFo 2019, 57 ff.

28 Vgl. *Hülsberg/Fassbach*, WPg im IDW Verlag, 2021, 1098 ff.

29 Vgl. *Rudolph*, StraFo 2019, 57 ff.

30 Vgl. *Hartung*, in: Wieland/Steinmeyer/Grüninger (Hrsg.), Handbuch Compliance-Management, 3. Aufl. 2020, S. 295 ff.

31 Vgl. Ziffer 4.5 IOA STANDARDS OF PRACTICE, hier abrufbar: https://www.ombudsassociation.org/assets/docs/IOA_Standards_of_Practice_Oct09.pdf.

des Landgerichts Bochum etwa den Grundsatz der Datensparsamkeit beachten. Soweit möglich, sollten sie keine beschlagnahmefähigen Dokumente und Daten herstellen bzw. innerhalb Deutschlands solche vorhalten. Ergebnisse lassen sich dem Unternehmen auch mündlich präsentieren, was sich in Anbetracht der Nichtgeltung von § 97 StPO für Dokumente außerhalb des anwaltlichen Gewahrsams ohnehin empfehlen kann. Ähnliches hat sich beispielsweise auch seit längerem bei der Kooperation mit US-amerikanischen Behörden etabliert; diesen werden häufig lediglich mündliche Zusammenfassungen von Berichten und Interviews präsentiert (sog. readouts und oral downloads).[32]

Rieder und *Menne* sehen eine Alternative zum vollständigen Verzicht auf Aufzeichnungen darin, auf die Verwendung physischer Dokumente zu verzichten und Informationen nur noch in digitaler Form auf ausländisch belegenen Servern zu verwalten. Digitalisiertes Vorgehen dürfte bei vielen Untersuchungen heutzutage ohnehin schon weitgehend Standard sein. Sofern im Falle einer Durchsuchung keine freiwillige Offenlegung der Zugänge erfolgt, dürfte ein darauf gerichtetes Herausgabeverlangen gegenüber Berufsgeheimnisträgern gemäß § 95 Abs. 2 StPO nicht zwangsweise durchgesetzt werden. Die Herausgabepflicht gilt nicht für Personen, die zur Verweigerung des Zeugnisses berechtigt sind. Auch *Rudolph* rät dazu, dass Compliance-Ombudsleute alle Informationen sicher verschlüsselt speichern, weil die Nennung des Passworts der anwaltlichen Schweigepflicht unterliegt.[33] Moderne Verschlüsselungsmethoden spielen eine entscheidende Rolle in der IT-Sicherheit. Passwörter sind für Ermittlungsbehörden nur schwer zu entschlüsseln. Die IT-Sicherheit stellt neben einem im Ausland belegenen Serverstandort eine effektive weitere „Line of Defense" dar. Ein absoluter Schutz besteht auch bei Verwendung ausländischer Server nicht, soweit die Daten im Rahmen entsprechender Rechtshilfeersuchen und -abkommen erlangt werden können. Zumindest im Hinblick auf kanzleieigene Server in Jurisdiktionen mit umfassenderem „legal privilege" dürfte dieses Risiko aber überschaubar sein. Zudem dürfte der Zugriff der Staatsanwaltschaft auf diese Weise faktisch erheblich erschwert oder zumindest verzögert sein.[34]

In der Konsequenz kann eine Enttarnung der Identität des Hinweisgebers durch deutsche Strafverfolgungsbehörden mit Hilfe eines im Ausland gehosteten internetbasierten anonymen Hinweisgebersystem verhindert beziehungsweise wesentlich erschwert werden. Die Ombudsperson erhält damit selbst keine Kenntnis von der Identität des Hinweisgebers, kann aber ggf. unberechtigte Vorwürfe bereits im Vorfeld klären und bei berechtigten, verfolgenswerten Vorwürfen eine Vertrauensperson für den Hinweisgeber sein. Internetbasierte Hinweisgebersysteme ermöglichen die Einbeziehung des Hinweisgebers in den weiteren Verlauf der Ermittlungen, ohne dass dieser seine Identität preisgeben muss. Hinweisgeber und Vertrauensanwalt greifen von ihren jeweiligen Standorten auf den Server zu. Dabei wird lediglich der Inhalt der Meldungen gespeichert, nicht aber die IP-Adresse oder sonstige Metadaten. Eine technische Rückverfolgung des Hinweises basierend auf den gespeicherten Daten ist daher unmöglich. Der Datentransfer zwischen Benutzer und Server erfolgt verschlüsselt, unterliegt aber darüber hinaus nicht dem Einflussbereich des Technologieanbieters, weshalb der Benutzer besonders darauf achten sollte, seine Anfragen von einem sicheren Endgerät aus zu tätigen. Die anonyme Kommunikation zwischen Hinweisgeber und Ombudsmann erfolgt über ein geschütztes Postfach. Zur Einrichtung des Postfachs muss der Hinweisgeber lediglich ein Pseudonym und ein Kennwort auswählen. Der Hinweisgeber muss zudem selbst darauf achten, dass er keine Informationen preisgibt, die Rückschlüsse auf seine Person zulassen.[35]

Worst-Case-Szenario für den Hinweisgeber ist der Fall, dass die Staatsanwaltschaft vom Vertrauensanwalt Zugang zu dem Passwort des internetbasierten anonymen Hinweisgebersystems erlangt. Wie aber kann das sein? Das Passwort unterliegt der anwaltlichen Schweigepflicht des Vertrauensanwalts. Eine spezifische Regelung im Mandatsvertrag sieht zudem die Verpflichtung des Auftraggebers vor, den Vertrauensanwalt nur mit Zustimmung des Hinweisgebers von der anwaltlichen Schweigepflicht zu entbinden. Diese Regelung wirkt aber nur im Verhältnis der Parteien des Mandatsvertrages. Es gilt die strikte Parteibindung des Mandatsvertrags. Die Entbindung von der Schweigepflicht ist eine rechtsgestaltende Erklärung, die schuldrechtlich unzulässig, weil vertragswidrig sein mag, aber in jedem Fall wirksam ist. Der Auftraggeber kann den Vertrauensanwalt somit jederzeit von der anwaltlichen Schweigepflicht entbinden. Dann steht einem Zugriff der Staatsanwaltschaft auf das Zeugenwissen des Vertrauensanwalts nichts mehr entgegen. Der Vertrauensanwalt muss in der Folge gegenüber der Staatsanwaltschaft das Passwort benennen. Motiv des Unternehmens für ein solches Vorgehen könnte die Hoffnung sein, dass eine umfassende Kooperation mit den Ermittlungsbehörden Berücksichtigung bei der Bemessung der gegen das Unternehmen gerichteten Geldbuße finden könnte („Cooperation Credit"). Soweit bekannt, haben Staatsanwaltschaften diesbezüglich noch kein Druck auf Unternehmen ausgeübt. Womöglich deshalb nicht, weil die Ermittlungsbehörden wissen, dass internetbasierte anonyme Hinweisgebersysteme dann nicht mehr als sicher gelten würden. Immerhin haben die Behörden solche Systeme selbst im Einsatz.

VI. Lösungsansätze

Hinweisgeber können zum Zwecke der Anonymitätssicherung einen eigenen Anwalt mandatieren, der die Hinweise für den gegenüber dem Unternehmen anonym bleibenden Hinweisgeber weitergibt und allein nur die Interessen des Hinweisgebers vertritt. In diesem Mandatsverhältnis sind Unterlagen beschlagnahmefrei. In den U. S. A. sind anwaltliche Vertreter für Hinweisgeber üblich. Hintergrund sind Belohnungen für Hinweisgeber, die sich auf diese Weise einen eigenen Anwalt auch leisten können. Beispiel: Mit einer Rekord-Belohnung von 200 Mio. USD haben sich die amerikanischen Ermittlungsbehörden bei einem Hinweisgeber der Deutschen Bank bedankt. Der Banker hat entscheidend dazu beigetragen, die Manipulationen des Libor-Zinssatzes aufzuklären.[36] Finanzielle Anreize für Hinweisgeber werden neuerdings auch in Deutschland befürwortet.[37]

De lege ferenda sollte der deutsche Gesetzgeber aber (auch) an der vertraglichen Beziehung zwischen Unternehmen und Vertrauensanwalt anknüpfen. Der Mandatsvertrag wird in der Literatur als Vertrag

32 Vgl. *Rieder/Menne*, CCZ 2018, 203 ff.
33 Vgl. *Rudolph*, StraFo 2019, 57 ff.
34 Vgl. *Rieder/Menne*, CCZ 2018, 203 ff.
35 Vgl. *Fassbach/Hülsberg*, GWR 2020, 255 ff.
36 Vgl. *Kanning*, FAZ v. 22.10.2021, hier abrufbar: https://www.faz.net/aktuell/finanzen/deutsche-bank-whistleblower-bekommen-200-millionen-dollar-175 97319.html.
37 Vgl. *Granetzny/Krause*, CCZ 2020, 29 ff.

zugunsten Dritter nach § 328 BGB eingeordnet.[38] Sinn und Zweck der EU-WBRL erfordert einen wirksamen Hinweisgeberschutz. Die bedeutet auch, dass die Anonymitätssicherung durch Vertrauensanwälte auch gegenüber den Strafverfolgungsbehörden funktionieren muss. Andernfalls wird der Vertrag zugunsten Dritter zur Makulatur. Ein „sicherer Raum" für Hinweisgeber erfordert legislative Sicherheit.

VII. Zusammenfassung

Die Wahrung der Anonymität ist für den Hinweisgeberschutz elementar. Jedem Hinweisgeber ist dringend anzuraten, seine Identität gegenüber dem Unternehmen nicht preiszugeben und ggf. zum Zwecke der Anonymitätssicherung einen eigenen Anwalt zu mandatieren. Ermittlungsbehörden und Gerichte können sich mit Hilfe einer Durchsuchung und Beschlagnahme beim Unternehmen jederzeit Kenntnis von der Identität des Hinweisgebers verschaffen. In der Konsequenz können Unternehmen den Hinweisgebern die Vertraulichkeit ihrer Identität nicht zusagen. Zum Schutz der Identität des Hinweisgebers sollten Vertrauensanwälte auf die Verwendung beschlagnahmefähiger physischer Dokumente verzichten und Informationen nur in digitaler Form auf im Ausland belegenen Servern verwalten. Eine Enttarnung der Identität des Hinweisgebers durch deutsche Strafverfolgungsbehörden kann mit Hilfe eines im Ausland gehosteten internetbasierten anonymen Hinweisgebersystems faktisch erheblich erschwert oder zumindest verzögert werden. Dann haben deutsche Ermittlungsbehörden nur im Rahmen entsprechender Rechtshilfeersuchen und -abkommen Zugriff auf die Daten und können diese ggf. entschlüsseln. Ein solches Katz-und-Mausspiel kann nicht im Sinne der EU-Whistleblower-Richtlinie sein. Der Appell an den Gesetzgeber lautet daher: Ohne Anonymitätssicherung ist ein wirksamer Hinweisgeberschutz nicht denkbar.

AUTOREN

Dr. Burkhard Fassbach *ist als Rechtsanwalt in eigener Praxis in Frankfurt am Main tätig. Nach einer Promotion im US-amerikanischen Reorganisationsrecht bei Prof. Dr. Manfred Wolf an der Johann Wolfgang Goethe-Universität ist er seit vielen Jahren in den Bereichen Compliance, Organhaftung und D&O-Versicherung spezialisiert.*

Dr. Frank Hülsberg *ist Wirtschaftsprüfer und Steuerberater. Er ist Mitglied des Vorstands bei Grant Thornton und verantwortet das Ressort Technology & Innovation. Zudem leitet er den Beratungsbereich Governance, Risk, Compliance & Technology. Seine Schwerpunkte liegen hier auf Wirtschaftskriminalität, Cyber Security, Data Analytics, Prozessdigitalisierung sowie IT-Strategieberatung und -umsetzung.*

Prof. Dr. Hansgeorg Spamer *ist als Rechtsanwalt in der mittelständisch geprägten Kanzlei Kummer Mehler Spamer Rechtsanwälte in Frankfurt am Main und Neu-Isenburg tätig. Er ist gelernter Bankkaufmann sowie seit rund zwanzig Jahren Fachanwalt für Arbeitsrecht. Von 2012 bis 2021 lehrte er zudem als Professor für Bürgerliches Recht und Arbeitsrecht an der Technischen Hochschule Aschaffenburg. Prof. Dr. Spamer ist auf die Bereiche Arbeitsrecht und Prozessführung spezialisiert.*

38 Vgl. *Goers*, Der Ombudsmann als Instrument unternehmensinterner Kriminalprävention, Frankfurt am Main, 2009, S. 40.