Julia Bakaus Lars-Heiko Kruse (Hg.)

Die „Zentrale Stelle“ in Kreditinstituten

Anti-Financial Crime in der Praxis

Frankfurt School
Verlag

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.

Besuchen Sie uns im Internet: http://www.frankfurt-school-verlag.de

ISBN (print): 978-3-95647-109-4
ISBN (pdf): 978-3-95647-110-0
ISBN (epub): 978-3-95647-111-7
ISBN (mobi): 978-3-95647-112-4

1. Auflage 2019 © Frankfurt School Verlag / efiport GmbH, Adickesallee 32-34, 60322 Frankfurt am Main

Einsatz von Hinweisgebersystemen

Albrecht Vahl

1 Einleitung

2 Gründe für Hinweisgebersysteme
2.1 Allgemeine Gründe
2.2 Rechtliche Gründe

3 Vorfragen zur Einrichtung von Hinweisgebersystemen

4 Unterschiedliche Hinweisgebersysteme

5 Kriterien für die Auswahl eines Hinweisgebersystems
5.1 Vorgehensweise
5.2 Übergreifende Kriterien
5.3 Kriterien für interne Systeme
5.4 Kriterien für externe Systeme
5.5 Kombinationen

6 Weitere Anforderungen
6.1 Datenschutz
6.2 Betriebsrat, Personalrat

7 Akute Krisenfälle

8 Ziel: Prävention und Aufklärung durch Vertrauen in die Vertraulichkeit

9 Ergebnis

Literatur

1 Einleitung

Betrug, Diebstahl, Unterschlagung, Korruption, Datenklau – Mitarbeiter und Externe haben viele Möglichkeiten, ein Unternehmen zu schädigen. Und dies passiert täglich. Die dadurch verursachten materiellen Schäden sind immens und werden allein für Deutschland auf bis zu 100 Mrd. EUR pro Jahr geschätzt,[1] wobei der einzelne Schadensfall bei Banken und Finanzdienstleistern mit durchschnittlich rund 6,8 Mio. EUR[2] beziffert wird. Hinzu kommen noch die immateriellen Schäden, insbesondere der Reputationsschaden, der beim betroffenen Unternehmen regelmäßig zu erheblich höheren Auswirkungen im Verhältnis zu Kunden, Geschäftspartnern, Behörden und Mitarbeitern führt.

Jede Branche und jede Hierarchieebene kann von Wirtschaftskriminalität betroffen sein. Und obwohl die Dunkelziffer bei diesen Regelverstößen bis zu 90% betragen soll, wird in den Medien laufend über neue Fälle und die betroffenen Unternehmen berichtet.

Die Gefährdung des Unternehmenserfolgs durch Regelverstöße ist latent vorhanden. Deshalb haben sich seit Jahren die Anforderungen an das Risikomanagement der Unternehmen und deren Sorgfaltspflichten kontinuierlich erhöht. Infolgedessen wurden die organisatorischen Pflichten immer genauer definiert. Dies hat dazu geführt, dass als Teil des Risikomanagements ausdrücklich auch die Betrugsprävention gefordert wird.

2 Gründe für Hinweisgebersysteme

Nach den Erkenntnissen der Ermittlungs- und der Aufsichtsbehörden sowie der Wirtschaftsprüfungsgesellschaften sind bei rund der Hälfte aller Fälle von Wirtschaftskriminalität interne Täter, also Mitarbeiter, beteiligt – und einzelne Kollegen wundern sich über Sonderlichkeiten. Dennoch herrscht großes Schweigen, selbst wenn sich konkrete Verdachtsmomente ergeben, weil alle Mitarbeiter grundsätzlich sehr loyal gegenüber Vorgesetzten und Kollegen sind.[3] Sie fürchten aber auch Repressalien, wenn sie ihre Bedenken offen aussprechen würden, oder haben die Sorge, nicht ernst genommen zu werden.

---

[1] KPMG AG, Wirtschaftskriminalität in Deutschland 2016 und 2018; Gemäß Bundeslagebilder Wirtschaftskriminalität des Bundeskriminalamts: 2017: 3,7 Mrd. EUR, 2016: 3,0 Mrd. EUR, 2015: 2,9 Mrd. EUR, 2014: 4,6 Mrd. EUR., s.a. Bundeslagebild Korruption 2017.

[2] PricewaterhouseCoopers AG/Martin-Luther-Universität Halle-Wittenberg, Wirtschaftskriminalität – Banken und andere Finanzdienstleister, März 2015.

[3] PricewaterhouseCoopers AG/Martin-Luther-Universität Halle-Wittenberg, Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2016 und Wirtschaftskriminalität 2018, Mehrwert von Compliance – forensische Erfahrungen.

Ziel eines Hinweisgebersystems ist es, das Schweigen von aufmerksamen Kollegen zu ändern und die Hemmschwelle für Hinweise zu minimieren, um die Prävention gegen strafbare Handlungen und sonstige Regelverstöße sowie deren Aufklärung zu erreichen.

2.1 Allgemeine Gründe

Jeder im Unternehmen – die Geschäftsleitung und die Mitarbeiter – hat ein Interesse daran, dass der Arbeitgeber nicht geschädigt wird – letztlich werden Arbeitsplätze gesichert, wenn Schädigungen des Instituts vermieden werden. Auch kleine Schadensfälle gilt es zu verhindern, denn sie sind häufig der erste Schritt zu größerem Fehlverhalten und können zu Abhängigkeiten sowie Schäden führen, die grundsätzlich alle treffen. Zur Verhinderung und zur Aufklärung von Schadensfällen ist ein Hinweisgebersystem – das zeigt die Praxis – ein gut geeignetes Instrument. Hierdurch lassen sich zusätzlich zu den bestehenden firmeninternen Berichtswegen[4] Informationen und Verdachtsmomente über Risiken und Fehlverhalten im Unternehmen leichter nutzbar machen, sodass Schäden verhindert oder zumindest verringert werden.

Voraussetzung ist, dass das Hinweisgebersystem im Unternehmen transparent geregelt und offensiv kommuniziert wird sowie dass Vertraulichkeit garantiert ist. Eine gute Basis dafür ist eine Unternehmenskultur der Offenheit, des Vertrauens und der Transparenz. Abhängig von der Ausgestaltung ist das Hinweisgebersystem ein Beleg dafür, wie stark ein Unternehmen an der Aufdeckung von Missständen im eigenen Unternehmen interessiert ist.[5]

Die häufig geäußerte Sorge, dass Hinweisgebersysteme zur – selbstverständlich unerwünschten – Denunziation von Kollegen führen, ist erfahrungsgemäß unbegründet.

Es ist die klare Tendenz zu erkennen, dass Hinweisgebersysteme bzw. Whistleblowing weiter zunehmen werden. Für jedes Unternehmen wird es sich auch positiv auswirken, wenn dort ein die Vertraulichkeit wahrendes Hinweisgebersystem eingeführt wird. Dadurch wird eine offensive, interne Kommunikation von Risiken gefördert, den Mitarbeitern wird das Signal gegeben, dass Rechtstreue sowie redliches Verhalten ausdrücklich erwünscht sind und es werden zudem Anreize zur Selbstkontrolle und Selbstreinigung gegeben. Darüber hinaus wird im Außenverhältnis die Reputation des Unternehmens gefördert.

[4] Bericht an Vorgesetzte, Compliance-Officer, Revision, Geschäftsleiter, Aufsichtsrat, Betriebsrat etc.

[5] Konstanz Institut für Corporate Governance – KICG Compliance Essentials 7/2017, 24.

Schließlich wird die – unerwünschte – Möglichkeit minimiert, dass der Whistleblower mittels Presse, Internet und sozialer Netzwerke seinen Hinweis öffentlich macht, und damit die Reputation des Unternehmens geschädigt wird. Die Schaffung eigenständiger interner Regeln für die Risikokommunikation innerhalb des Unternehmens ist der bessere Weg. Denn ohne ein eingerichtetes Hinweisgebersystem ist die Wahrscheinlichkeit höher, dass Mitarbeiter ihre Hinweise entweder verschweigen oder extern veröffentlichen. Aufgrund der Angst der Mitarbeiter vor Repressalien dient die Einrichtung eines Hinweisgebersystems auch dem Interesse der Mitarbeiter und dem Betriebsfrieden, weil damit ein geregelter Umgang mit Hinweisen zu Missständen geschaffen wird.

Hinzu kommt, dass jedes durch einen Hinweis erkannte Risiko durch organisatorische Maßnahmen für die Zukunft minimiert, jede durch einen Hinweis bekannt gewordene Schwäche der Ablauforganisation beseitigt und jeder Regelverstoß verfolgt sowie der Täter eher in Anspruch genommen werden kann.

Zudem ist die präventive Wirkung eines Hinweisgebersystems beachtlich: Der potenzielle Täter muss befürchten, dadurch entdeckt zu werden, weshalb er ggf. schon deshalb von seinem unredlichen Vorhaben Abstand nimmt.[6]

Eine ausdrückliche gesetzliche Verpflichtung, ein Hinweisgebersystem einzuführen, gibt es seit Jahren in den USA für Firmen, die an der Börse notiert sind.[7] Dagegen wurde das Thema in Deutschland sehr zurückhaltend behandelt.[8] Zwar empfehlen die internationalen und die nationalen Handelskammern schon seit 2008 die Einrichtung von Hinweisgebersystemen zur Verhinderung von Korruption.[9] Aber es bedurfte meist großer, öffentlichkeitswirksamer Fälle von Wirtschaftskriminalität, die dazu führten, dass Unternehmen Hinweisgebersysteme installiert haben.[10]

2.2 Rechtliche Gründe

Die Geschäftsleitung ist verpflichtet, für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen.

[6] Schemmel/Ruhmannseder/Witzigmann, Hinweisgebersysteme: Implementierung in Unternehmen, 2012, 317.

[7] Siehe Sarbanes-Oxley Act (SOX), Section 301, von 2002.

[8] Am 18. Juni 2015 wurde der Gesetzesentwurf zum Schutz von Hinweisgebern vom Deutschen Bundestag abgelehnt.

[9] Siehe Internationale Handelskammer (ICC), Ein ICC-Verhaltenskodex für die Wirtschaft, Deutscher Industrie- und Handelskammertag (DIHT).

[10] So z.B. Deutsche Bahn, Siemens etc.

In Folge der Finanzmarktkrise ist seit 2013 eine Vielzahl von gesetzlichen Vorschriften zur Erweiterung der Internen Kontrollsysteme (IKS), der Compliance-Management-Systeme (CMS) einschließlich einer Verschärfung der Strafvorschriften und ausdrücklich auch zur Einrichtung von Hinweisgebersystemen erlassen worden.

Seit Januar 2014 gelten die „Besonderen organisatorischen Pflichten" gemäß § 25a Abs. 1 Kreditwesengesetz (KWG), wonach eine ordnungsgemäße Geschäftsorganisation von Instituten einen Prozess umfasst, der es den Mitarbeitern unter Wahrung der Vertraulichkeit ihrer Identität ermöglicht, Gesetzesverstöße und etwaige strafbare Handlungen innerhalb des Unternehmens an geeignete Stellen zu berichten. Mit dieser Vorschrift wurde ein Hinweisgebersystem in Deutschland erstmals – wenn auch zunächst nur für Institute im Sinne des KWG – gesetzlich normiert.

Mit Inkrafttreten des neuen Geldwäschegesetzes (GwG) in 2017 wurden auch hier Vorschriften zu den internen Sicherungsmaßnahmen kodifiziert. Demnach müssen die dem GwG Verpflichteten gemäß § 6 Abs. 5 GwG im Hinblick auf ihre Art und Größe angemessene Vorkehrungen treffen, damit es ihren Mitarbeitern und Personen in vergleichbaren Positionen unter Wahrung der Vertraulichkeit ihrer Identität möglich ist, Verstöße gegen geldwäscherechtliche Vorschriften an geeignete Stellen zu berichten. Diese Formulierung entspricht weitgehend dem § 25a Abs. 1 KWG. Auch die Aufsichtsbehörden werden hier entsprechend verpflichtet (§ 53 Abs. 1, 3 GwG).

Ergänzend gelten die Auslegungs- und Anwendungshinweise gemäß § 51 Abs. 8 GwG der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), die die seit 2011 gültigen Auslegungs- und Anwendungshinweise der Deutschen Kreditwirtschaft zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen ganz oder teilweise abgelöst haben.[11] Hierin war bereits formuliert, dass die Schaffung eines internen oder externen niedrigschwelligen Informationsweges, der die Anonymität von Mitarbeitern sicherstellt (z.B. Hinweisgebersystem bzw. Whistleblowing), bei der Aufdeckung strafbarer Handlungen hilfreich sein kann.[12]

Vergleichbare Regelungen wurden vom Parlament der Europäischen Union (EU) in verschiedenen Bereichen verabschiedet und wurden bzw. werden in nationales Recht umgesetzt, z.B.:

[11] Auslegungs- und Anwendungshinweise gem. § 51 Abs. 8 GWG, Ziff. 3.8. Whistleblowing, vom 11. Dezember 2018.

[12] Auslegungs- und Anwendungshinweise der Deutschen Kreditwirtschaft zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und „sonstigen strafbaren Handlungen" vom 16. Dezember 2011, Stand: 1. Februar 2014, Ziff. 89, Seite 86.

- Marktmissbrauchsverordnung und -richtlinie: Arbeitgeber/Emittenten von Finanzinstrumenten oder Akteure des Marktes für Emissionszertifikate müssen angemessene interne Verfahren einrichten, über die ihre Mitarbeiter Verstöße intern melden können.[13] Das konkretisieren § 25h KWG und die Mindestanforderungen an das Risikomanagement (MaRisk).[14] Die Mitgliedsstaaten können finanzielle Anreize für Hinweisgeber gewähren.[15] Dementsprechend wurde das Erste Finanzmarktnovellierungsgesetz am 30. Juni 2016 verkündet.[16]
- Nach der Richtlinie betreffend Organismen für gemeinsame Anlagen in Wertpapieren (OGAW V) sind in den Verwaltungsgesellschaften, Investmentgesellschaften und Verwahrstellen für die Meldung von Verstößen Verfahren einzurichten, wonach die Mitarbeiter Verstöße intern über einen speziellen, unabhängigen und autonomen Kanal melden können.[17] Ferner sind die Vertraulichkeit zu garantieren und der Schutz der personenbezogenen Daten sicherzustellen. Dementsprechend wurde das OGAW-V-Umsetzungsgesetz am 3. März 2016 verkündet.[18]
- Die Geldtransferverordnung verlangt von den Zahlungsdienstleistern Verfahren einzurichten, über die insbesondere ihre Mitarbeiter Verstöße gegen die Verordnung über einen sicheren, unabhängigen, spezifischen und anonymen Weg melden können.[19]
- Nach der Verordnung bzgl. der Aufsicht über Kreditinstitute durch die Europäische Zentralbank (EZB) sorgt die EZB dafür, dass wirksame Mechanismen für die Meldung von Verstößen durch Kreditinstitute eingerichtet werden, einschließlich spezieller Verfahren für die Entgegennahme von Meldungen. Der angemessene Schutz der

[13] Art. 32, Abs. 3 der Verordnung (EU) Nr. 596/2014 des europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung).

[14] BaFin, Rundschreiben 09/2017 (BA) vom 27. Oktober 2017 „Mindestanforderungen an das Risikomanagement – MaRisk".

[15] Art. 32, Abs. 4 Marktmissbrauchsverordnung.

[16] Erstes Gesetz zur Novellierung von Finanzmarktvorschriften auf Grund europäischer Rechtsakte (Erstes Finanzmarktnovellierungsgesetz – 1. FiMaNoG) vom 30. Juni 2016, BGBl. vom 1. Juli 2016.

[17] Art. 99d der Richtlinie 2014/91/EU des europäischen Parlaments und des Rates vom 23. Juli 2014 (OGAW-V-Richtlinie).

[18] OGAW-V-Umsetzungsgesetz vom 03. März 2016, BGBl. vom 10. März 2016.

[19] Art. 21 Abs. 2 der Verordnung (EU) 2015/847 des europäischen Parlaments und des Rates vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU) Nr. 1781/2006 (neue Geldtransferverordnung, gültig seit 26. Juni 2017).

meldenden Person, der beschuldigten Person und der personenbezogenen Daten ist zu gewährleisten.[20]

Auch im Finanzdienstleistungsaufsichtsgesetz (FinDAG) ist geregelt, dass die BaFin ein System zur Annahme von Meldungen über Verstöße gegen Gesetze und sonstige Vorschriften errichtet. Die Identität der meldenden und der betroffenen Personen wird von der BaFin geschützt; dieser Schutz gilt jedoch ausdrücklich nicht, wenn eine Weitergabe der Information im Kontext weiterer Ermittlungs- oder Gerichtsverfahren erforderlich ist. Die meldende Person darf weder nach arbeitsrechtlichen oder strafrechtlichen Vorschriften verantwortlich gemacht noch zum Ersatz von Schäden herangezogen werden, es sei denn, die Meldung ist vorsätzlich oder grob fahrlässig unwahr abgegeben worden.[21] Dementsprechend wurde bei der BaFin eine Hinweisgeberstelle installiert. Darüber hinaus wurde ein internetbasiertes anonymes System eingeführt.

Ebenso haben gemäß Börsengesetz (BörsG) die Börsenaufsichtsbehörde (§ 3b) und der Börsenträger (§ 5 Abs. 8) entsprechende Regelungen zur Meldung von Verstößen zu treffen.

Gleiches gilt für Kapitalverwaltungsgesellschaften gem. §§ 28 Abs. 1 Nr. 9, 68 Abs. 4, 119 Abs. 6 Kapitalanlagegesetzbuch (KAGB).

Ebenfalls ist im Wertpapierhandelsgesetz (WpHG) zusätzlich zum allgemeinen Verweis auf § 25a KWG für Datenbereitstellungsdienste die Pflicht zur Einführung von Hinweisgebersystemen geregelt.[22]

Ferner steht im Versicherungsaufsichtsgesetz, dass es den Mitarbeitern zu ermöglichen ist, Regelverstöße unter Wahrung der Vertraulichkeit ihrer Identität an eine geeignete Stelle zu melden (§ 23 Abs. 6 VAG, s.a. § 34d Abs. 12 Gewerbeordnung).

Schließlich gilt Entsprechendes für Wirtschaftsprüfer, die Abschlussprüfungen durchführen (§ 55b Abs. 2 Nr. 7 Wirtschaftsprüferordnung).

[20] Art. 23 der Verordnung (EU) Nr. 1024/2013 des Rates vom 15. Oktober 2013 zur Übertragung besonderer Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute auf die Europäische Zentralbank (SSM-VO) sowie Art. 36 der Verordnung EZB/2014/17 der Europäischen Zentralbank vom 16. April 2014 zur Einrichtung eines Rahmenwerks für die Zusammenarbeit zwischen der Europäischen Zentralbank und den nationalen zuständigen Behörden und den nationalen benannten Behörden innerhalb des einheitlichen Aufsichtsmechanismus (SSM-RahmenVO).

[21] § 4d Gesetz über die BaFin – FinDAG vom 30. Juni 2016. Dies beruht auf § 53 GwG.

[22] § 80 Abs. WpHG und ausdrücklich für Veröffentlichungssysteme (§ 58 Abs. 6), Bereitsteller konsolidierter Datenticker (§ 59 Abs. 5), Meldemechanismen (§ 60 Abs. 5).

Das Gesetz zum Schutz von Geschäftsgeheimnissen (§ 5 GeschGehG) schützt seit April 2019 Hinweisgeber, die im öffentlichen Interesse Fehlverhalten offenlegen.

Gemäß dem Deutschen Corporate Governance Kodex soll im Sinne eines Best-Practice-Compliance-Management-Systems den Beschäftigten auf geeignete Weise die Möglichkeit eingeräumt werden, geschützt Hinweise auf Rechtsverstöße im Unternehmen zu geben; Dritte sollten als mögliche Hinweisgeber einbezogen werden.[23]

Nach allem ist zusätzlich zu berücksichtigen, dass der Vorstand und die Geschäftsführung sowie das jeweilige Aufsichtsgremium mit der Einführung eines umfassenden Risikomanagementsystems einschließlich eines Hinweisgebersystems die Gefahr minimieren, wegen eigener Organisationsfehler strafrechtlich belangt oder auf Schadensersatz in Anspruch genommen zu werden und an persönlicher Reputation zu verlieren. Dies gilt auch für die zuständigen leitenden Angestellten.

Nach der sog. Konsultationsphase hat die Europäische Kommission darüber hinaus am 23. April 2018 einen Richtlinienvorschlag zum Schutz von Whistleblowern vorgelegt. Dieser verfolgt zum einen die Pflicht, Kommunikationskanäle für Hinweisgeber zu schaffen (Art. 1 I, 4, 6 RL-Vorschlag), zum anderen den Schutz von Hinweisgebern (Art. 13-15 RL-Vorschlag). Inhaltlich sieht der Vorschlag ein dreistufiges Meldesystem vor:

Zunächst soll sich der Hinweisgeber an interne Meldekanäle wenden. Sollten diese internen Kanäle nicht funktionieren oder nach vernünftigem Ermessen nicht funktionieren können, so besteht die Möglichkeit zur externen Meldung an zuständige Behörden (sog. externer Meldekanal, Art. 6-12 RL-Vorschlag). Wenn nach einer Meldung über den internen bzw. externen Meldekanal keine geeigneten Maßnahmen ergriffen worden sind oder wenn eine unmittelbare oder offenkundige Gefährdung des öffentlichen Interesses oder die Gefahr eines irreparablen Schadens besteht, sieht der Vorschlag als ultima ratio Meldungen in der Öffentlichkeit oder den Medien vor.[24]

[23] Ziff. 4.1.3, S. 3 Deutscher Corporate Governance Kodex in der am 07. Februar 2017 beschlossenen Fassung, veröffentlicht im Bundesanzeiger am 24. April 2017, siehe www.dcgk.de, vgl. Entsprechenserklärung gem. § 161 AktG. In der künftigen Neufassung des Kodex wird dies voraussichtlich in Grundsatz 7, A.3 geregelt.

[24] Europäische Kommission, Konsultation der Europäischen Kommission zum Schutz von Whistleblowern vom 3.März 2017, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54254; Europäische Kommission, Richtlinienvorschlag COM(2018) 218 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, vom 23.04.2018, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:52018PC0218&qid=1555406343090. Schmolke, Der Vorschlag für eine europäische Whistleblower-Richtlinie, AG 2018, 769.

Mit Pressemitteilung hat das Europäische Parlament im März 2019 bekannt gegeben, dass es sich mit dem Rat auf Regeln zum besseren Schutz von Whistleblowern geeinigt hat.[25] Die vorläufige Vereinbarung muss von den Botschaftern der Mitgliedstaaten (AStV)[26] und dem Rechtsausschuss bestätigt werden, bevor sie von Plenum und Rat endgültig verabschiedet wird.

3 Vorfragen zur Einrichtung von Hinweisgebersystemen

Bevor bei der Planung der Einführung eines Hinweisgebersystems die Details zu verschiedenen Arten von Hinweisgebersystemen geprüft werden, sind insbesondere folgende Vorfragen zu beantworten:

- Soll nur die Muttergesellschaft ein Hinweisgebersystem erhalten?
- Soll das Hinweisgebersystem zentral oder dezentral eingerichtet werden?
- Wer soll Hinweise geben – nur Mitarbeiter (Interne) oder auch Lieferanten etc. (Externe, Dritte)?
- Zu welchen Themen sollen Hinweise gegeben werden?
- Werden auch anonyme Hinweise bearbeitet?

Insoweit ist eine individuelle Abwägung geboten. Einschränkungen ohne besondere Gründe erscheinen nicht zielführend, Hinweisgebersysteme sollten einen einheitlichen und offenen Kommunikationskanal anbieten.

Ein potenzieller Hinweisgeber kennt meist nur einen kleinen Ausschnitt des Sachverhalts, er kann die Relevanz und Bedeutung oft nicht vollständig einschätzen, hat aber Anhaltspunkte oder einen Verdacht oder ein Störgefühl, wonach „da etwas nicht mit rechten Dingen zugeht". Jeder Hinweis kann wertvoll sein; die Bedeutung eines Hinweises lässt sich regelmäßig nicht zu Beginn, sondern erst am Ende der Untersuchung bewerten. Auch risikoorientierte Ansätze funktionieren nur bedingt, weil regelmäßig keine Erfahrungswerte vorliegen.[27]

[25] Europäisches Parlament, Pressemitteilung vom 12. März 2019, Referenz-Nr.: 20190311IPR31055.

[26] Ausschuss der Ständigen Vertreter der Regierungen der Mitgliedstaaten der Europäischen Union.

[27] Der Kapitän der Titanic, E. J. Smith (1850-1912), soll gesagt haben: „Ich bin 40 Jahre auf hoher See unfallfrei gefahren und habe mich nie in einer misslichen Situation befunden." (Quelle unbekannt).

Allerdings bietet es sich meist an, spezifische Personalthemen, z.B. bezüglich Gehalt, Beförderung, zwischenmenschliche Beziehungen etc., vom Hinweisgebersystem fernzuhalten. Gleichwohl müssen solche Themen ebenfalls betriebsintern abgearbeitet werden, denn auch ein Vorwurf wegen angeblichen Mobbings kann durch einen Korruptionsfall bedingt sein.

Auch das Allgemeine Gleichbehandlungsgesetz (AGG) ist zu beachten. Es kann sinnvoll sein, die Beschwerdestelle i.S.v. § 13 AGG ebenfalls dem Hinweisgebersystem anzugliedern.

4 Unterschiedliche Hinweisgebersysteme

Das Unternehmen kann unterschiedliche Hinweisgebersysteme einrichten. Beim internen System sollen die Hinweise z.B. an den Compliance-Officer oder eine interne Hotline erfolgen, während bei einem externen System die Hinweise an eine externe Stelle, etwa an ein internetbasiertes Meldewesen oder an einen Ombudsmann[28] gerichtet werden. Es gilt also wie folgt zu unterscheiden:

- interne Hinweisgebersysteme:
  - Meldestelle für telefonische Hinweise,
  - Meldestelle für schriftliche Hinweise per E-Mail oder via Intranet,
  - Briefkasten für schriftliche Hinweise,
  - Ansprechpartner Compliance-Officer,
  - Ansprechpartner Syndikusanwalt;
- externe Hinweisgebersysteme:
  - Telefonhotline,
  - elektronische Systeme,
  - Ombudsperson bzw. Ombudsfrau, Ombudsmann.[29]

[28] Ausschuss der Ständigen Vertreter der Regierungen der Mitgliedstaaten der Europäischen Union.

[29] Zur vereinfachten Darstellung wird im Folgenden nur der am meisten gebräuchliche Begriff „Ombudsmann“ verwendet.

5 Kriterien für die Auswahl eines Hinweisgebersystems

5.1 Vorgehensweise

Es ist zu entscheiden, welches Hinweisgebersystem für das Unternehmen zu bevorzugen ist.

5.2 Übergreifende Kriterien

Übergreifend sollten die folgenden Kriterien bei der Entscheidungsfindung herangezogen werden:

- Vertraulichkeit,
- Anonymität,
- Erreichbarkeit,
- elektronische Kommunikation (einschl. Verschlüsselung),
- Möglichkeit des persönlichen Gesprächs,
- Rückfragen und Rückmeldung,
- transparente Verfahrensabläufe, die Vertrauen schaffen,
- Fremdsprachenabdeckung,
- Kosten.

Anerkanntermaßen hängt die Effektivität des Hinweisgebersystems elementar davon ab, in welchem Umfang dem Hinweisgeber Vertraulichkeit und Anonymität gewährleistet wird und ob dies für den Hinweisgeber auch nachvollziehbar und glaubhaft gemacht wird.

Insofern bestehen gegen Hinweisgebersysteme, die die Datenverarbeitung über das Internet oder das Intranet nutzen, bei den potenziellen Hinweisgebern regelmäßig Bedenken gegen die Vertraulichkeit, die Anonymität und den Datenschutz, weil sich elektronische Kommunikation nicht 100%ig sicher schützen lässt und die Angriffe auf die elektronische Datenverarbeitung laufend zunehmen. Technisch hochentwickelte Cyberangriffe sind inzwischen sehr ernst zu nehmender Alltag.[30]

[30] BaFin Newsletter vom 16. März 2017 bezüglich IT-Aufsicht bei Banken, Bundesamt für Sicherheit in der Informationstechnik (BSI), Lagebericht zur IT-Sicherheit 2018.

5.3 Kriterien für interne Systeme

Zusätzlich zu den in Abschnitt 5.2 aufgeführten Punkten ist für interne Systeme zu berücksichtigen, dass betriebsinterne Themen möglichst intern bleiben sollten. Deshalb ist ein internes System grundsätzlich sinnvoll. In der Praxis hat sich jedoch gezeigt, dass nur sehr wenige Hinweise an die internen Systeme gegeben werden. Dies ist v.a. unter Berücksichtigung der Kriterien der Vertraulichkeit und der Anonymität zu erklären. Um die Effektivität des Hinweisgebersystems zu steigern, ist das interne System um eine externe Komponente zu erweitern.

5.4 Kriterien für externe Systeme

Zusätzlich zu den in Abschnitt 5.2 aufgeführten Punkten ist für externe Systeme die überwiegend vertretene Meinung zu berücksichtigen, dass die Hemmschwelle, die der Hinweisgeber zu überwinden hat um einen Hinweis zu geben, bei einem externen System etwas geringer ist als bei einem internen System. Ansonsten sind für die folgenden unterschiedlichen Ausprägungen externer Systeme entsprechende Unterscheidungsmerkmale zu berücksichtigen.

Externe Hotlines

Verschiedene nationale und internationale Dienstleister bieten zur Entgegennahme von Hinweisen auf Regelverstöße in unterschiedlicher Ausgestaltung Call-Center an. Im Einzelfall sind die Leistungen an den in Abschnitt 5.2 genannten Kriterien zu messen.

Externe elektronische Systeme

Verschiedene nationale und internationale Dienstleister bieten zur Entgegennahme von Hinweisen auf Regelverstöße in unterschiedlicher Ausgestaltung internetbasierte Meldewege an. Dazu zählt z.B. das in internationalen und nationalen Wirtschaftsunternehmen sowie in Behörden im In- und Ausland installierte Business-Keeper-Monitoring-System (BKMS).[31]

Die herausragende Besonderheit dieser elektronischen Systeme ist die täglich 24-stündige Erreichbarkeit an 365 Tagen jährlich. Im Einzelfall sind die Leistungen an den in Abschnitt 5.2 genannten Kriterien zu messen.

[31] Siehe Beitrag von Leisering.

Ombudsmann

Der Ombudsmann kann den Sachverhalt ausführlich und pragmatisch mit dem Hinweisgeber besprechen und wird erst nach ausdrücklicher Freigabe durch den Hinweisgeber und unter Wahrung der Identität des Hinweisgebers die zuständige Stelle im betroffenen Unternehmen informieren.[32]

Der Erstkontakt zum Ombudsmann erfolgt meistens telefonisch. Es ist sofort und im Verlauf des weiteren Verfahrens möglich, Rückfragen direkt an den Hinweisgeber zu stellen. Dadurch kann die Plausibilität frühzeitig überprüft und die Glaubwürdigkeit des Hinweisgebers eingeschätzt sowie ein gegenseitiges Vertrauensverhältnis aufgebaut werden. Ferner sind konkrete Nachfragen zum Sachverhalt möglich und zu Details, die sich manchmal erst im Verlauf der internen Untersuchung ergeben. Soweit sachdienlich, können persönliche Vier-Augen-Gespräche geführt sowie Dokumente und Datenträger vertraulich gesichtet und ggf. ausgetauscht werden.

Der direkte Kontakt von Mensch zu Mensch ermöglicht transparente Verfahrensabläufe und kann für den Hinweisgeber die Berührungsängste beseitigen sowie das Vertrauen in die Vertraulichkeit fördern, um einen sachdienlichen Informationsaustausch im Interesse des Unternehmens zu ermöglichen.

Ein weiteres wesentliches Kriterium ist, dass der Ombudsmann im Einzelfall zur Wahrung der Vertraulichkeit eigene Recherchen durchführen kann, z. B. bei der Auswertung von Unterlagen oder Daten, die Rückschlüsse auf die Person des Hinweisgebers zulassen könnten. Dieses Beweismaterial kann zur Aufklärung des aktuellen Sachverhalts und für künftige Präventionsmaßnahmen wichtig sein, selbst wenn der Ombudsmann dieses Beweismaterial im Einzelfall zum Schutz des Hinweisgebers nicht weitergeben darf.

Vor allem kann ein Ombudsmann, der als Rechtsanwalt zugelassen und selbstständig tätig ist, ein sehr hohes Vertrauen in die Vertraulichkeit gewährleisten:

- Der anwaltliche Ombudsmann ist gesetzlich zur Verschwiegenheit zum Schutz der Mandantschaft verpflichtet. Dies ist mit dem Unternehmen als Auftraggeber vertraglich ausdrücklich zu Gunsten des Hinweisgebers zu vereinbaren.
- Der anwaltliche Ombudsmann kann sich – soweit im Einzelfall relevant – gegenüber den staatlichen Ermittlungsbehörden auf sein Aussageverweigerungsrecht berufen.

Entgegen der bisher einhelligen Meinung ist streitig geworden, ob ein Rechtsanwalt, der im Auftrag eines Unternehmens als Ombudsmann tätig ist, sich in einem staatsanwalt-

[32] Informationen für Hinweisgeber, www.ombudsmann-vahl.de.

schaftlichen Ermittlungsverfahren zum Schutz des Hinweisgebers auf ein Beschlagnahmeverbot berufen kann. In einem Beschluss des Landgerichts Bochum wird eine Beschlagnahme von Unterlagen beim Ombudsmann für rechtens gehalten.[33] Dies wird in der Literatur mit guter Begründung kritisiert.[34] Eine höchstrichterliche Entscheidung liegt bisher nicht vor.

Unabhängig von dieser streitigen Rechtsfrage wird der anwaltliche Ombudsmann demnach – sofern im speziellen Einzelfall die Beschlagnahme von Unterlagen überhaupt relevant werden könnte – entsprechend sorgfältig agieren.

Die oben genannten zusätzlichen europäischen Regelungen werden einen einheitlichen Rechtsrahmen für ein hohes Schutzniveau und die Unterstützung von Hinweisgebern ermöglichen.

Auf das Privileg des Beschlagnahmeverbots kann sich ein Syndikusanwalt jedenfalls nicht berufen.[35]

Ferner ist es nicht zielführend, als Ombudsmann den Firmenanwalt, der das Unternehmen in anderen Rechtsgebieten berät, zu beauftragen. Insbesondere wenn der Rechtsanwalt im Personalrecht berät oder weitergehende Beratungsmandate von der Geschäftsführung hat, ist eine Interessenkollision nicht auszuschließen. Dies gilt umso mehr aus der Sicht eines potenziellen Hinweisgebers.

Schließlich kann der anwaltliche Ombudsmann im Einzelfall sowohl gegenüber dem Hinweisgeber als auch gegenüber dem Unternehmen, ergänzend zu den in Abschnitt 5.2 genannten Kriterien, juristisch qualifizierte Ratschläge geben.

5.5 Kombinationen

Kombinationen ergeben sich zwingend, da bereits bei den rein internen Hinweisgebersystemen mehrere mögliche Ansprechpartner für einen Hinweisgeber vorhanden

[33] Landgericht Bochum, Beschluss vom 16. März 2016, II-6 Qs 1/16, NStZ 2016, 500.

[34] Schmid/Wengenroth, (Keine) Beschlagnahmefreiheit für Compliance-Ombudspersonen, NZWiSt 2016, 401 (404 ff.), Queling/Bayer, Beschlagnahmeverbot im Hinweisgebersystem unter Einsatz von Ombudsanwälten, NZWiSt 2016, 417, Frank/Vogel, Beschlagnahmefreiheit für Unterlagen anwaltli-cher Compliance-Ombudspersonen, NStZ 2017, 313, Egger, Hinweisgebersysteme und Informantenschutz, CCZ 2018, 126, Baranowski/Pant, Die janusköpfigen Verschwiegenheitsrechte und –pflichten des Rechtsanwalts in der Funktion einer Ombudsperson, CCZ 2018, 250.

[35] EuGH-Urteil C-550/07 P vom 14. September 2010 (Akzo Nobel Kartellverfahren).

sind.[36] Kommt als zusätzlicher Baustein ein Modul aus den möglichen externen Meldewegen hinzu, ergibt sich aus dieser Kombination eine Chance und sogar eine Pflicht zur Zusammenarbeit und zum Informationsaustausch. Dadurch können atypische Entwicklungen und besondere Häufungen (z.B. auch aus dem Bereich der Kundenbeschwerden oder der Personalabteilung) erkannt und ausgewertet werden.

Die Installation eines externen Hinweisgebersystems als zusätzlichem Baustein führt nicht zu einer Auslagerung i.S.v. § 25h Abs. 4 KWG.

In Einzelfällen kann es auch angebracht sein, spezielle Meldewege zu kombinieren, insbesondere ein elektronisches System (intern oder extern) mit einem Ombudsmann. Gründe dafür können sein:

- hohe Zahl von Mitarbeitern mit unterschiedlichen Qualifikationen;
- viele Unternehmensstandorte;
- Inlands- und Auslandsbezug mit Zeitverschiebungen und mehreren Fremdsprachen;
- Besonderheiten in der Kombination der betroffenen inländischen und ausländischen Rechtsordnungen, insbesondere im Arbeitsrecht und Datenschutz.

In diesem Sinne können z.B. internationale Unternehmen, die in der Unternehmensgruppe ein internationales elektronisches Hinweisgebersystem installiert haben, im Inland für die Mitarbeiter aber einen Ombudsmann als Ansprechpartner für vertrauliche Hinweise nutzen.

6 Weitere Anforderungen

6.1 Datenschutz

Das Unternehmen hat den Schutz der persönlichen Daten der Mitarbeiter, die von einem Hinweis betroffen sind, ebenso wie die ggf. bekannten Daten des Hinweisgebers gesetzeskonform sicherzustellen. Nach den allgemein gehaltenen Vorschriften im deutschen Datenschutzrecht ist das Abwägen der gegenseitigen Interessen aller Beteiligten im Einzelfall geboten, aber auch zulässig. Ferner können ausdrückliche Regelungen in speziel-

[36] Zusätzlich zu den üblichen Berichtswegen, siehe oben Fußnote 4.

len Gesetzen sowie ausländische Rechtsordnungen mit besonderen Anforderungen zu berücksichtigen sein.[37]

Auch der externe Dienstleister muss den Datenschutz zugunsten der Beteiligten sicherstellen.

6.2 Betriebsrat, Personalrat

Die Einführung eines Hinweisgebersystems, das es dem Mitarbeiter ermöglicht, Hinweise auf unredliches Verhalten zu melden, ohne dass für die Mitarbeiter eine Pflicht zur Meldung vorgeschrieben wird, ist zwar grundsätzlich nicht mitbestimmungspflichtig.[38] Jedoch ist es mindestens im Sinne der Glaubwürdigkeit, der Transparenz und der gemeinsamen Interessenslage sinnvoll, die Mitarbeitervertretung bei der Einführung eines Hinweisgebersystems frühzeitig einzubeziehen, um größtmögliche Akzeptanz zu erreichen.

7 Akute Krisenfälle

In einem akuten Krisenfall, der intern erhebliche Auswirkungen haben kann oder sogar schon in der Presse öffentlich gemacht wurde, ist es erforderlich, besondere Sofortmaßnahmen zu ergreifen. Zur Vertiefung und Beschleunigung der Sachverhaltsaufklärung und zur Verbesserung der Reputation ist es häufig sinnvoll, ein Hinweisgebersystem – soweit noch nicht vorhanden – kurzfristig einzurichten bzw. zu erweitern, z.B. mit einem externen Baustein, eventuell zunächst nur befristet.

In solchen Fällen bietet sich vor allem ein anwaltlicher Ombudsmann an, weil er schnell als qualifizierter und persönlicher Ansprechpartner den Mitarbeitern zur Verfügung stehen kann und nur ein geringer organisatorischer Aufwand für die Einrichtung eines Hinweisgebersystems mit Ombudsmann nötig ist.

[37] Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines, Datenschutzkonferenz vom 14. November 2018.

[38] § 87 Abs. 1 Betriebsverfassungsgesetz und § 75 Abs. 3 Bundespersonalvertretungsgesetz, siehe auch BAG NZA 2008, 1248 (Honeywell-Fall).

8 Ziel: Prävention und Aufklärung durch Vertrauen in die Vertraulichkeit

Das entscheidende Kriterium für den Erfolg eines Hinweisgebersystems ist das Vertrauen der potenziellen Hinweisgeber in die Zuverlässigkeit des Systems. Und weil der Hinweisgeber typischerweise große Angst vor Repressalien und dem Verlust seines Arbeitsplatzes hat, muss das Vertrauen des Hinweisgebers in die Vertraulichkeit des Hinweisgebersystems an erster Stelle stehen.

Dieses Vertrauen muss sich das Unternehmen sowohl bei der Installation des Hinweisgebersystems als auch anschließend kontinuierlich nachhaltig erarbeiten sowie bei der Bearbeitung von Hinweisen bestätigen.[39] Dadurch kann das Ziel, im Unternehmen einerseits durch Prävention strafbare Handlungen und sonstige Regelverstöße zu vermeiden und andererseits aufzuklären, erreicht werden.

9 Ergebnis

Die Sorge vor Hinweisgebersystemen als mögliche Quelle für Denunziation ist unbegründet. Hinweisgebersysteme können die Beteiligten schützen. Insbesondere für Kreditinstitute und andere Finanzdienstleistungsunternehmen sowie nach dem Geldwäschegesetz ist die Einführung eines Hinweisgebersystems Pflicht; für weitere Unternehmen wird sie es werden.

Darüber hinaus kann künftig im gesamten Wirtschaftsleben und für jedes Konzern- oder Tochterunternehmen die Best Practice des Risikomanagements mit der Schaffung eines Hinweisgebersystems oder dessen verbesserte Ausgestaltung zur Kür werden. Im Einzelfall sind die unterschiedlichen Kriterien der verschiedenen Hinweisgebersysteme abzuwägen.

[39] Miege, Einrichtung eines Hinweisgebersystems, CCZ 2018, 45.

Tabelle 1: Auswahlkriterien für Hinweisgebersyssteme

Art des Hinweisgebersystems	Interne Hinweisgebersysteme				Externe Hinweisgebersysteme		
Auswahlkriterien	Internes Telefon, E-Mail, Intranet	Briefkasten	Mitarbeiter aus Compliance, Recht, Revision etc.	Syndikusanwalt	Externe Telefon-Hotline	Externes elektronisches System	Rechtsanwalt als Ombudsmann
Vertraulichkeit	-	+	0	0	0	+	+
Anonymität	-	+	-	-	0	+	+
Erreichbarkeit	0	0	0	0	0	+	0
Elektronische Kommunikation einschl. Verschlüsselung	-	-	0	0	-	+	+
Möglichkeit des persönlichen Gesprächs	+	-	+	+	0	-	+
Vertrauliche Prüfung von Unterlagen und Daten	-	-	0	0	-	-	+
Rückfragen und Rückmeldung	+	-	+	+	+	+	+
Transparente Verfahrensabläufe, die Vertrauen schaffen	-	0	0	0	0	0	+
Aussageverweigerungsrecht	-	-	-	-	-	Entfällt	+
Beschlagnahme von Akten oder Daten	-	-	-	-	-	-	0
Fremdsprachenabdeckung	0	+	0	0	+	+	0
Kosten	+	+	+	0	+	0	0
_____							
_____							

Zeichenerklärung: + = gut/positiv, 0 = mittel/neutral, - = schlecht/negativ

Literatur

BaFin, Rundschreiben 09/2017 (BA) vom 27. Oktober 2017 „Mindestanforderungen an das Risikomanagement – MaRisk".

BaFin, Auslegungsentscheidung vom 11. Dezember 2018, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz.

BaFin Newsletter vom 16. März 2017 bezüglich IT-Aufsicht bei Banken, www.bafin.de/dok/9051704.

Baranowski, Carolin/Pant, Benjamin, Die janusköpfigen Verschwiegenheitsrechte und –pflichten des Rechtsanwalts in der Funktion einer Ombudsperson, CCZ 2018, 250.

Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2018, September 2018, abrufbar unter https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.

Bundesarbeitsgericht, Beschl. vom 22. Juli 2008, Az.: 1 ABR 40/07, NZA 2008, 1248 (Honeywell-Fall).

Bundeslagebilder Wirtschaftskriminalität 2015 bis 2017 des Bundeskriminalamts, abrufbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Wirtschaftskriminalitaet/wirtschaftskriminalitaet_node.html.

Bundeslagebilder Korruption 2017 des Bundeskriminalamts, Stand Mai 2018, abrufbar unter https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Korruption/korruptionBundeslagebild2017.html.

Deutsche Kreditwirtschaft, Auslegungs- und Anwendungshinweise der Deutschen Kreditwirtschaft zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und „sonstigen strafbaren Handlungen" vom 16. Dezember 2011, Stand: 1. Februar 2014, veröffentlicht durch das BaFin-Rundschreiben 1/2014 (GW) vom 5. März 2014 (zuletzt geändert am 10. November 2014): Verwaltungspraxis zu den gesetzlichen Vorschriften zur Verhinderung von Geldwäsche und Terrorismusfinanzierung im Geldwäschegesetz und Kreditwesengesetz, abrufbar unter https://die-dk.de/kontofuehrung/geldwaescheverhinderung.

Egger, Mathes, Hinweisgebersysteme und Informantenschutz, CCZ 2018, 126.

Europäische Zentralbank, Verordnung EZB/2014/17 der Europäischen Zentralbank vom 16. April 2014 zur Einrichtung eines Rahmenwerks für die Zusammenarbeit zwischen der Europäischen Zentralbank und den nationalen zuständigen Behörden und den nationalen benannten Behörden innerhalb des einheitlichen Aufsichtsmechanismus (SSM-RahmenVO).

Europäischer Gerichtshof, Urteil C-550/07 P vom 14. September 2010 (Akzo Nobel Kartellverfahren).

Europäischer Rat, Verordnung (EU) Nr. 1024/2013 des Rates vom 15. Oktober 2013 zur Übertragung besonderer Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute auf die Europäische Zentralbank (SSM-VO).

Europäisches Parlament und Rat, Richtlinie 2014/91/EU des europäischen Parlaments und des Rates vom 23. Juli 2014 zur Änderung der Richtlinie 2009/65/EG zur Koordinierung der Rechts- und Verwaltungsvorschriften betreffend bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (OGAW) im Hinblick auf die Aufgaben der Verwahrstelle, die Vergütungspolitik und Sanktionen (OGAW-V-Richtlinie).

Europäisches Parlament und Rat, Verordnung (EU) 2015/847 des europäischen Parlaments und des Rates vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU) Nr. 1781/2006.

Europäisches Parlament und Rat, Verordnung (EU) Nr. 596/2014 des europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission.

Frank/Vogel, Beschlagnahmefreiheit für Unterlagen anwaltlicher Compliance-Ombudspersonen, NStZ 2017, 313.

Internationale Handelskammer (ICC), Ein ICC-Verhaltenskodex für die Wirtschaft, abrufbar unter http://www.icc-deutschland.de/fileadmin/ICC_Dokumente/ICC-Verhaltenskodex_Korruption_final.pdf.

Grüninger, Stefan/Wanzek, Matthias/Wiebe, Anna (2017): Compliance Essentials – Was aus der Perspektive von Justiz, Verbänden und Unternehmen wirklich zählt, Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG); Konstanz Institut für Corporate Governance (KICG) (Hg.), Konstanz, abrufbar unter https://www.htwg-konstanz.de.

KPMG AG Wirtschaftsprüfungsgesellschaft, Wirtschaftskriminalität in Deutschland 2016 und 2018, abrufbar unter https://home.kpmg.com/de/de/home/themen/2016/07/wirtschaftskriminalitaet-2016.html und https://home.kpmg.com/de/de/home/newsroom/press-releases/2018/07/wirtschaftskriminalitaet-in-deutschland-2018.html.

Landgericht Bochum, Beschluss vom 16. März 2016, II-6 Qs 1/16, NStZ 2016, 500.

Miege, Christian, Einrichtung eines Hinweisgebersystems, CCZ 2018, 45.

Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines, Datenschutzkonferenz, 14. November 2018, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf.

PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft/Martin-Luther-Universität Halle-Wittenberg Wirtschaftskriminalität 2018, Mehrwert von Compliance – forensische Erfahrungen, abrufbar unter https://www.pwc.de/de/risk/pwc-wikri-2018.pdf.

PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft/Martin-Luther-Universität Halle-Wittenberg, Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2016, abrufbar unter https://www.pwc.de/de/risk/studie-wirtschaftskriminalitaet-2016.pdf.

PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft/Martin-Luther-Universität Halle-Wittenberg, Wirtschaftskriminalität Banken und andere Finanzdienstleister, März 2015.

Queling, André/Bayer, Sarah, Beschlagnahmeverbot im Hinweisgebersystem unter Einsatz von Ombudsanwälten, NZWiSt 2016, 417.

Sarbanes-Oxley Act (SOX), Section 301, 2002.

Schemmel, Alexander/Ruhmannseder, Felix/Witzigmann, Tobias, Hinweisgebersysteme: Implementierung in Unternehmen, 2012.

Schmid, Alexander/Wengenroth, Lenard, (Keine) Beschlagnahmefreiheit für Compliance-Ombudspersonen, NZWiSt 2016, 401 (404 ff.).

Schmolke, Klaus Ulrich, Der Vorschlag für eine europäische Whistleblower-Richtlinie, AG 2018, 769.

Vahl, Albrecht, Informationen für Hinweisgeber, https://www.ombudsmann-vahl.de.