

Corporate Whistleblowing

ZHR 181 (2017) 847–860

I. Einleitung

Es gibt kaum einen Bereich im Unternehmensrecht, der in den letzten Jahren so stark weiterentwickelt und ausgebaut wurde wie Corporate Compliance. Auch wenn dieser Begriff im Aktiengesetz gar nicht vorkommt, werden die damit verbundenen organisatorischen Fragen in allen Kommentaren zum AktG und mehreren Handbüchern ausführlich behandelt. Der Grundgedanke ist einfach: Es geht um die selbstverständliche Aufgabe der Unternehmensleitung, dafür zu sorgen, dass die bestehenden Gesetze und Regeln, von denen das Unternehmen betroffen ist, auch befolgt werden. Bei der Frage, wie dies geschehen soll, ob dafür eine spezielle Compliance-Organisation einzurichten ist und was dazu im Einzelnen gehört, bestehen allerdings Meinungsverschiedenheiten. Schon die Frage, ob überhaupt eine Compliance-Pflicht besteht, wird unterschiedlich beantwortet. Ein Teilaspekt dieser Diskussion ist die Frage, ob die Unternehmen verpflichtet sind, ein System bereitzustellen, über das Mitarbeiter und eventuell auch Außenstehende offen oder anonym auf Regelverletzungen im Unternehmen hinweisen können (sog. *Whistleblowing*). Der Deutsche Corporate Governance Kodex (DCGK) enthält in seiner neuesten Fassung erstmals die Empfehlung, eine solche Möglichkeit einzuräumen.¹ Die Empfehlung richtet sich an alle börsennotierten Gesellschaften. Ihre Beachtung wird darüber hinaus auch den nicht kapitalmarktorientierten Gesellschaften empfohlen.² Die EU-Kommission hatte die börsennotierten Gesellschaften bereits 2005 ermahnt zu überprüfen, ob ihre Arbeitnehmer die Möglichkeit haben, mutmaßliche Unregelmäßigkeiten in der Gesellschaft durch Beschwerden oder anonyme Mitteilungen an ein unabhängiges Mitglied der Unternehmensleitung anzuzeigen.³ Diese Empfehlung ist in Deutschland ohne erkennbare Resonanz geblieben. Grund dafür war vermutlich der Umstand, dass die Empfehlung an die Prüfungsausschüsse gerichtet war, die im

1 Ziff. 4. 1. 3 S. 3 DCGK i.d.F. v. 7. 2. 2017.

2 Vgl. Präambel, vorletzter Abs. DCGK.

3 Vgl. Anhang I Ziff. 4. 3. 8 der Empfehlung der Kommission vom 15. 2. 2005 zu den Aufgaben von nicht geschäftsführenden Direktoren/Aufsichtsratsmitgliedern/börsennotierter Gesellschaften sowie zu den Ausschüssen des Verwaltungs-/Aufsichtsrats, ABl. EU Nr. L 52 v. 25. 2. 2005, S. 51.

deutschen dualistischen System als Teil des Aufsichtsrates zwar für die Überwachung der Compliance, nicht aber für die Einführung bestimmter Prozesse zuständig sind.

II. Gesetzliche Grundlagen

Den deutschen Gesellschaften, deren Aktien an der New Yorker Börse gelistet sind, ist das sog. *Whistleblowing* spätestens seit dem Sarbanes-Oxley Act von 2002 vertraut. Danach sind internationale Unternehmen verpflichtet, eine vertrauliche und anonyme Meldemöglichkeit für Hinweise zu fragwürdigen Bilanzierungsmethoden einzurichten.⁴ Durch den Dodd Frank Act von 2010 wurde diese Regelung dahin erweitert, dass finanzielle Anreize für Hinweisgeber eingeführt wurden.⁵ Falls eine Information zu einer Geldbuße von mehr als 1 Mio USD führt, ist die SEC verpflichtet, dem Hinweisgeber eine Belohnung von 10 bis 30 % der verhängten Geldbuße auszuhändigen (sog. *Bounty-Program*). *Bradley Birkenfeld*, ein Mitarbeiter der Schweizer Großbank UBS, konnte 2014 aus dem entsprechenden Programm der US Steuerbehörde Internal Revenue Service eine Belohnung in Höhe von 104 Mio USD vereinnahmen.⁶

Die Einrichtung eines Whistleblowing- oder Hinweisgebersystems ist seit einiger Zeit auch in mehreren deutschen Gesetzen vorgeschrieben. So sieht z.B. § 25a Abs. 1 S. 6 Nr. 3 KWG vor, dass eine ordnungsgemäße Geschäftsorganisation von Instituten einen Prozess umfasst, der es den Mitarbeitern unter Wahrung der Vertraulichkeit ihrer Identität ermöglicht, Verstöße gegen bestimmte EU-Verordnungen, das KWG und die dazu erlassenen Rechtsverordnungen sowie etwaige strafbare Handlungen innerhalb des Unternehmens an geeignete Stellen zu berichten.⁷ Entsprechende Bestimmungen sind in § 23 Abs. 6 VAG für die Versicherungsunternehmen und in § 28 Abs. 1 S. 2 Nr. 9 KAGB für Kapitalverwaltungsgesellschaften enthalten. Auch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ist gemäß § 4d FinDAG⁸ verpflichtet, ein System zur Annahme von Meldungen über potentielle oder tatsächliche Verstöße gegen Gesetze und sonstige Vorschriften zu errichten, bei denen es die Aufgabe der Bundesanstalt ist, deren Einhaltung sicherzustellen

4 Vgl. Sec. 301 SOX; der arbeitsrechtliche Schutz des Whistleblowers gemäß sec. 806 SOX gilt nur für Mitarbeiter in den USA.

5 Sec. 21F des Security Exchange Act i.d.F. des Dodd-Frank Wall Street Reform and Consumer Protection Act vom Juli 2010.

6 https://de.wikipedia.org/wiki/Bradley_Birkenfeld.

7 Vgl. auch die allgemeiner gehaltene Verpflichtung der Wertpapierdienstleistungsunternehmen zur Einrichtung einer wirksamen Compliance-Funktion gemäß § 33 Abs. 1 S. 2 Nr. 1 WpHG.

8 § 4d des Gesetzes über die Bundesanstalt für Finanzdienstleistungsaufsicht (Finanzdienstleistungsaufsichtsgesetz – FinDAG).

und Verstöße dagegen zu ahnden. Eine entsprechende Meldeplattform wurde am 2. 7. 2016 eingerichtet.⁹

Mit den Regelungen im KWG und VAG in der aktuellen Fassung wurde Art. 32 Abs. 1 und 3 der Marktmissbrauchs-Verordnung (MMVO) umgesetzt, wonach die EU-Mitgliedstaaten dafür sorgen sollen, dass die zuständigen Behörden und Arbeitgeber im Finanzdienstleistungsbereich angemessene Verfahren einrichten, um die Meldung von Verstößen gegen die Marktmissbrauchs-Verordnung zu ermöglichen. Art. 32 Abs. 4 MMVO stellt den Mitgliedstaaten darüber hinaus frei, für Informationen über mögliche Verstöße gegen die Verordnung finanzielle Anreize vorzusehen, sofern die bereitgestellten Informationen neu sind und zur Verhängung einer verwaltungs- oder strafrechtlichen Sanktion führen. Eine solche Möglichkeit hat der deutsche Gesetzgeber nicht vorgesehen. Dies kann nur begrüßt werden. Die Auslobung staatlicher „Fangprämien“ mag zwar tendenziell zu einer Erhöhung der Zahl von Meldungen führen. Sie birgt aber die Gefahr, dass gezielt nach Missständen gesucht wird und dadurch im Unternehmen eine Atmosphäre des allgemeinen Misstrauens entsteht.¹⁰

III. Empfehlung des DCGK

Die Regierungskommission Deutscher Corporate Governance Kodex hat die neuere Gesetzgebung offenbar verfolgt und daraus den Schluss gezogen, dass es sich beim *Whistleblowing* um einen bisher nicht aufgegriffenen Standard guter Unternehmensführung handelt und deshalb in Ziff. 4. 1. 3 S. 3 DCGK allen börsennotierten Gesellschaften die Einrichtung von Hinweisgebermöglichkeiten empfohlen. Beschäftigten soll auf geeignete Weise die Möglichkeit eingeräumt werden, geschützt Hinweise auf Rechtsverstöße im Unternehmen zu geben. Ergänzend wird angeregt, diese Möglichkeit auch Dritten einzuräumen. Dabei schwebt der Kommission als Ergänzung zum Compliance-Management-System die Einrichtung eines Hinweisgebersystems vor.¹¹ Diese Empfehlung wirft eine Reihe von Fragen auf, die im Folgenden kurz erörtert werden sollen.

1. Allgemeine Rechtspflicht zur Einrichtung eines Hinweisgebersystems?

Zunächst stellt sich die Frage, ob die börsennotierten Aktiengesellschaften nicht unabhängig von der Empfehlung des Kodex verpflichtet sind, ein Hinweisgebersystem einzurichten. Falls eine solche Pflicht bestehen sollte,

⁹ Vgl. www.bafin.de; zum Verfahren siehe die Verordnung zur Meldung von Verstößen gegen das Verbot der Marktmanipulation (Marktmanipulations-Verstoßverordnung – MarVerstMeldV) v. 2. 7. 2016, BGBl. I (2016), S. 1572.

¹⁰ Ablehnend auch C. Buchert, CCZ 2013, 144, 146 („Irrweg“).

¹¹ Vgl. die Erläuterungen der Änderungsvorschläge der Kommission aus der Plenarsitzung vom 13. 10. 2016.

würde die Empfehlung nur geltendes Recht wiederholen und wäre deshalb als Empfehlung überflüssig.

a) Entsprechende Anwendung des Aufsichtsrechts

Eine Pflicht der börsennotierten Gesellschaften zur Einrichtung eines Hinweisgebersystems könnte sich aus einer entsprechenden Anwendung der genannten Bestimmungen des Aufsichtsrechts ergeben. So wird schon seit einiger Zeit diskutiert, ob nicht die besonderen Organisationspflichten des KWG, VAG und WpHG eine normative „Ausstrahlung“ auf das Aktienrecht und insbesondere die allgemeinen Anforderungen an die Compliance haben.¹² Was diese „Ausstrahlung“ methodisch bedeutet, ist allerdings unklar. Eine generelle Übertragung der Organisationspflichten des Aufsichtsrechts auf das Aktienrecht scheidet schon deshalb aus, weil es sich beim Aufsichtsrecht um ein Sonderrecht für bestimmte Unternehmen handelt, die mit ihrer Geschäftstätigkeit eine besondere Verantwortung ihren Kunden und der Gesellschaft gegenüber tragen und für die deshalb spezielle Compliance-Vorgaben gelten. Die Compliance-Regelungen für diese Unternehmen können zwar Vorbild für Aktiengesellschaften außerhalb dieses Sonderrechts sein, sind für diese aber nicht ohne weiteres verbindlich.¹³ Das gilt insbesondere für Detailregelungen wie die Einrichtung eines Hinweisgebersystems.¹⁴

b) Verpflichtung aufgrund Aktienrecht

Unabhängig vom Aufsichtsrecht könnte auch das Aktiengesetz selbst die Einrichtung eines Hinweisgeber-Systems verlangen. So besteht weitgehend Einigkeit, dass den Vorstand aufgrund seiner allgemeinen Leitungspflicht (§§ 76 Abs. 1, 93 Abs. 1 AktG) eine Pflicht zur Compliance, also zu Vorkehrungen gegen mögliche Rechtsverletzungen des Unternehmens und seiner Mitarbeiter, trifft.¹⁵ Wie diese Vorkehrungen im Einzelnen aussehen, hängt allerdings von der Größe und Organisation des Unternehmens sowie dem Risikopotential seiner Geschäftstätigkeit ab.¹⁶ Bei der Ausgestaltung der Compliance im Unternehmen handelt es sich demgemäß nicht um die Umsetzung bestimmter gesetzlicher Vorgaben, sondern um eine Entscheidung, bei welcher

12 Vgl. dazu *Dreber*, ZGR 2010, 496 ff.; *Hopt*, ZGR 2013, 165, 205; *Kaetzler/Hoops*, BKR 2013, 192, 197; *Langenbacher*, ZHR 176 (2012) 652, 666 ff.

13 Vgl. *Bürkle*, WM 2005, 1496, 1497; *Spindler/Stilz/Fleischer*, AktG, 3. Aufl. 2015, § 91 AktG Rdn. 43; *KölnKommAktG/Mertens/Cahn*, 3. Aufl. 2009, § 91 AktG Rdn. 31; *Verse*, ZHR 175 (2011) 401, 403; *Baumbach/Hueck/Zöllner/Noack*, GmbHG, 21. Aufl. 2017, § 35 Rdn. 67.

14 Zurückhaltend auch *Spindler/Stilz/Fleischer* (Fn. 13), § 91 AktG Rdn. 61 zu den Details aufsichtsrechtlicher Vorgaben.

15 *Hüffer/Koch*, AktG, 12. Aufl. 2016, § 76 AktG Rdn. 12.

16 Vgl. *MünchKommAktG/Spindler*, § 91 AktG Rdn. 36; LG München NZG 2014, 345, 347.

dem Vorstand ein weites Organisationsermessen zusteht.¹⁷ Welche Maßnahmen im Einzelnen ergriffen werden, hängt wesentlich davon ab, wie der Vorstand deren Vor- und Nachteile für das Unternehmen einschätzt.

Zur Einrichtung eines Hinweisgeber-Systems wird im Schrifttum häufig betont, dass es sich dabei um ein „Kernelement“ der Compliance¹⁸ handele, das speziell bei börsennotierten Unternehmen zur „best practice von Compliance-Programmen“¹⁹ gehöre. Eine Rechtspflicht zur Einrichtung eines solchen Systems ergibt sich aus einer solchen Einschätzung allerdings nicht, auch wenn die meisten großen Gesellschaften schon seit etlichen Jahren eine interne oder externe Stelle zur Entgegennahme vertraulicher Hinweise auf Rechtsverstöße eingerichtet haben. Für die Frage einer Rechtspflicht kommt es vielmehr darauf an, in welchem Verhältnis der Nutzen einer solchen Einrichtung zu eventuellen Nachteilen steht.²⁰ Eine Rechtspflicht wäre nur dann zu bejahen, wenn die Voraussetzungen einer Ermessensreduzierung auf Null vorlägen.²¹

Der Nutzen eines Whistleblower-Systems wird vielfach darin gesehen, dass damit Risiken im Unternehmen früh erkannt werden.²² Insbesondere durch die Möglichkeit anonymer Meldungen kann den Mitarbeitern die Hemmschwelle genommen werden, um festgestellte oder vermutete Rechtsverletzungen im Unternehmen zu melden. Entsprechende Hinweise bleiben dabei im Unternehmen und können dort unter Ausschluss der Öffentlichkeit bearbeitet werden. In welchem Umfang aufgrund eines internen Hinweisgeber-Systems tatsächlich relevante Rechtsverletzungen im Unternehmen aufgedeckt werden, ist allerdings offen. Gesicherte Erkenntnisse liegen dazu nicht vor.²³ Eine Umfrage unter Schweizer Unternehmen aus dem Jahre 2012 hat ergeben, dass in der Regel weniger als zehn Meldungen jährlich abgegeben werden.²⁴ Bei den (wenigen) Unternehmen, bei denen über 100 Meldungen p.a.

17 Casper, Liber Amicorum, Winter, 2011, S. 77, 86; Hüffer/Koch (Fn. 15), § 76 AktG Rdn. 14; MünchKommAktG/Spindler (Fn. 16), § 91 AktG Rdn. 66.

18 Vgl. Maume/Haffke, ZIP 2016, 199, 200; Hauschka/Moosmayer/Lösler/R. Buchert, Corporate Compliance, 3. Aufl. 2016, § 42 Rdn. 4: „Herzstück eines Compliance-Management-Systems“; Schulz/Möhlenbeck, Compliance-Management im Unternehmen, 2017, 3. Kap. Rdn. 8: „elementarer Bestandteil eines effektiven Compliance-Management-Systems“.

19 Abraham, ZRP 2012, 11, 12.

20 Fleischer/Schmolke, WM 2012, 1013, 1016; Casper, Liber Amicorum Winter, 2011, S. 77, 88.

21 Fleischer/Schmolke, WM 2012, 1013, 1016.

22 So z.B. Hauschka/Moosmayer/Lösler/R. Buchert (Fn. 18), § 42 Rdn. 4.

23 Hauschka/Moosmayer/Lösler/R. Buchert (Fn. 18), § 42 Rdn. 4 Fn. 15. Casper, Liber Amicorum Winter, 2011, S. 77, 88 f.; Fleischer/Schmolke, WM 2012, 1013, 1017.

24 Vgl. die Angaben verschiedener Schweizer Unternehmen bei Rieder, Whistleblowing als interne Risikokommunikation: Ausgestaltung eines unternehmensinternen Whistleblowing-Systems aus arbeits- und datenschutzrechtlicher Sicht, 2013, S. 316, 321, 325, 330, 338, 341 und 347 mit jeweils unter 10 Meldungen pro Jahr.

eingingen, waren viele irrelevant oder betrafen Personalangelegenheiten.²⁵ Dieses Ergebnis deckt sich mit den Angaben von Seiten deutscher Gesellschaften. Dass ein Whistleblower-System zur Früherkennung wesentlicher Risiken verhilft, ist danach zwar nicht ausgeschlossen, aber eher die Ausnahme.

Dass die Einrichtung eines anonymen Meldekanals nicht dazu führt, dass ständig Hinweise auf Rechtsverstöße eingehen, ist nicht überraschend. Um die Unternehmen wäre es schlecht bestellt, wenn es anders wäre. Die Verantwortung für die bestmögliche Früherkennung von Rechtsverstößen liegt ohnehin nicht bei den Mitarbeitern, sondern bei den jeweiligen Compliance-Stellen und der Internen Revision. Die Bitte an die Mitarbeiter, ebenfalls aufmerksam zu sein und verdächtige Vorgänge zu melden, ist nur eine ergänzende Maßnahme. Ob dieser Bitte auch tatsächlich entsprochen wird, ist keineswegs sicher. Zwar könnte daran gedacht werden, die Mitarbeiter zur Meldung von erkannten oder vermuteten Rechtsverstößen einzelvertraglich oder über eine interne Richtlinie zu verpflichten. Ein solches Vorgehen würde der Mitbestimmung des Betriebsrats unterliegen (§ 87 Abs. 1 Nr. 1 BetrVG).²⁶ Die Auflegung einer generellen Rechtspflicht zum „Verpfeifen“ von Kollegen ist aber auch durch das Persönlichkeitsrecht der rechtstreuen Mitarbeiter begrenzt.²⁷ Allenfalls bei schwerwiegenden Straftaten mit erheblichen Folgen für das Unternehmen gebietet die Treuepflicht des Arbeitnehmers, dass der Arbeitgeber informiert wird.²⁸

Zu den offenkundigen Nachteilen eines Hinweisgeber-Systems gehört der damit verbundene Aufwand. Im Grundsatz genügen zwar die Einrichtung einer internetbasierten Meldeplattform und einer *Hotline* sowie die Bestimmung der für die Bearbeitung von Hinweisen zuständigen Stelle. Um ein System zu errichten, das möglichst alle Mitarbeiter im Unternehmen oder Konzern erreicht, ist häufig jedoch die Einrichtung mehrerer *Hotlines* erforderlich.²⁹ Ergänzend oder alternativ wird vielfach auch ein Ombudsmann bestellt. Auch hier kann es zweckmäßig sein, gleich mehrere Ombudsleute zu bestellen.³⁰ Dabei ist es angebracht, die Aufgaben solcher externen Anlaufstellen bei der Entgegennahme vertraulicher Hinweise und der Zusammenarbeit mit dem Unternehmen einschließlich der Vergütung vertraglich klar zu re-

25 Rieder (Fn. 24), S. 344, 350, 353.

26 Vgl. LAG Düsseldorf NZA-RR 2006, 81 ff. zur Wal-Mart Germany GmbH & Co. KG.

27 Casper, Liber Amicorum Winter, 2011, S. 77, 95.

28 Casper, Liber Amicorum Winter, 2011, S. 77, 95.

29 Die BASF SE hat z.B. gruppenweit 56 externe *Hotlines* eingerichtet, vgl. <http://bericht.basf.com/2016/de/corporate-governance/compliance.html>.

30 Die Volkswagen AG hat z.B. zwei externe Rechtsanwälte als Ombudsleute verpflichtet, vgl. <https://volkswagenag.com/de/group/compliance-and-risk-management/whistleblowing>.

geln.³¹ Insgesamt kann der Aufwand für ein Hinweisgeber-System erheblich sein.

Angesichts des schwer einschätzbaren Nutzens eines Hinweisgebersystems im Verhältnis zu dem damit verbundenen Aufwand kann auch aus der Sicht des AktG keine Rechtspflicht zur Einrichtung eines solchen Systems angenommen werden.³² Die Empfehlung des Kodex ist deshalb nicht überflüssig. Sie erscheint aber überzogen, weil sie alle börsennotierten Gesellschaften erfasst, ohne die unterschiedlichen Gegebenheiten dieser Unternehmen zu berücksichtigen. Kleinere Unternehmen sowie Unternehmen mit geringer Risikoexposition müssen schon keine institutionalisierten Compliance-Strukturen aufweisen.³³ Sie brauchen in der Regel auch kein Hinweisgebersystem. Der Vorstand kann sich stattdessen damit begnügen, das rechtstreue Verhalten der Mitarbeiter z.B. mit Hilfe von regelmäßigen Unterweisungen und einer offenen Gesprächskultur zu gewährleisten.³⁴ Bei einer offenen Gesprächskultur gehört es zum guten Ton, dass erkannte Missstände oder Rechtsverstöße dem jeweiligen Vorgesetzten oder der Compliance-Abteilung auch ohne Hinweisgeber-System mitgeteilt werden.³⁵ Werden entsprechende Hinweise auf Wunsch vertraulich behandelt und versehentlich falsche Hinweise nicht sanktioniert, reicht dies völlig aus, um auch die Mitarbeiter in die Früherkennung von Rechtsverstößen einzubinden. Die Einrichtung eines wie immer gearteten „Systems“ zur Erfassung und Bearbeitung anonymer Hinweise ist dazu nicht erforderlich. Eine „Speak up“-Kultur dürfte in vielen Fällen genauso effizient sein wie ein ausgefeiltes Hinweisgeber-System. Angesichts der Empfehlung des Kodex werden die börsennotierten Gesellschaften künftig allerdings bestrebt sein (müssen), die Anforderungen des Kodex zu erfüllen, um bei der externen Bewertung ihrer Corporate Governance möglichst gut abzuschneiden.

2. Gegenstand von Hinweisen

Vergleicht man die Empfehlung des Kodex mit den Meldesystemen, die in der Praxis bereits etabliert sind, so fällt auf, dass die Gegenstände, auf die sich die erwünschten Hinweise beziehen, unterschiedlich umschrieben werden. Bei den regulierten Unternehmen geht es darum, Verstöße gegen die einschlägigen Bestimmungen des Aufsichtsrechts und etwaige strafbare Handlungen im Unternehmen zu melden.³⁶ Der Kodex schlägt den Bogen dagegen weiter,

31 Zur Vertragsgestaltung näher Hauschka/Moosmayer/Lösler/R. Buchert (Fn. 18), § 42 Rdn. 113 ff.

32 Baur/Holle, AG 2017, 379, 379f.; Casper, Liber Amicorum Winter, 2011, S. 77, 88f.; Fleischer/Schmolke, WM 2012, 1013, 1017; Hüffer/Koch (Fn. 15), § 76 AktG Rdn. 18; Hauschka/Moosmayer/Lösler/R. Buchert (Fn. 18), § 42 Rdn. 62.

33 Hüffer/Koch (Fn. 15), § 76 AktG Rdn. 15.

34 Harbarth, ZHR 179 (2015) 136, 153.

35 Vgl. Krieger/Uwe H. Schneider/Kremer/Klahold, Handbuch Managerhaftung, 3. Aufl. 2017, § 25 Rdn. 25.47.

36 § 25a Abs. 1 S. 6 Nr. 3 KWG.

indem er potentiell alle Rechtsverstöße im Unternehmen unabhängig von ihrer Art und Schwere erfasst. In den Hinweissystemen einiger DAX-Gesellschaften wird demgegenüber nur zu Hinweisen auf „schwere Verstöße gegen Gesetze und interne Regelungen“ aufgerufen.³⁷ Auch eine thematische Schwerpunktsetzung wie z.B. Hinweise auf Kartellverstöße und Korruption ist möglich.³⁸ Eine solche Fokussierung kann durchaus sachgerecht sein, indem sie das Meldesystem auf für das Unternehmen wesentliche Verstöße ausrichtet. Entsprechende Regelungen sollten daher als ausreichende Befolgung der Kodex-Empfehlung akzeptiert werden. Keine Einschränkung des Meldegegenstands liegt dagegen vor, wenn darauf hingewiesen wird, dass das Hinweisgebersystem nicht für Beschwerden gedacht ist.³⁹ Das Beschwerderecht ist bereits in § 84 BetrVG geregelt und wird vom Kodex nicht erfasst.

3. Schutz des Hinweisgebers

Nach der Empfehlung in Ziff. 4.1.3 S. 3 DCGK sollen Beschäftigte und ggf. auch Dritte die Möglichkeit haben, „geschützt“ Hinweise auf Rechtsverstöße im Unternehmen zu geben. Was mit diesem Schutz gemeint ist und wie dieser aussehen soll, wird nicht näher bestimmt. Gemeint könnte sein, dass Hinweisgeber Gelegenheit haben sollen, etwaige Hinweise auch anonym geben zu können, ohne ihre Identität offen legen zu müssen. Die Zusicherung der Anonymität kann Mitarbeiter ermutigen, etwaige Kenntnisse von Rechtsverstößen weiterzugeben, ohne dadurch Nachteile befürchten zu müssen. Der Schutz eines Hinweisgebers ist in den meisten Fällen aber auch dann gewährleistet, wenn er zwar seine Identität offenlegen muss, ihm aber zugesichert wird, dass diese vertraulich behandelt wird. Dies ist das übliche Verfahren bei der Einschaltung einer externen Ombudsstelle. Dieser Schutz sollte als Befolgung der Kodex-Empfehlung ausreichen. So verlangen auch die eingangs erwähnten aufsichtsrechtlichen Bestimmungen nur, dass die Vertraulichkeit der Identität des Hinweisgebers gewährleistet ist.⁴⁰

Die Frage nach dem Schutz des Hinweisgebers geht aber weiter. Erweist sich z.B. ein Hinweis als unberechtigt, so ist der Hinweisgeber geschützt, wenn er anonym tätig geworden ist. Wurde dem Hinweisgeber dagegen, z.B. von einem Ombudsmann, nur die Vertraulichkeit seiner Identität zugesichert, kann diese Vertraulichkeit bei wissentlich oder leichtfertig unwahren Angaben nachträglich aufgehoben und der Hinweisgeber zur Rechenschaft gezogen werden. Die Zusicherung der Vertraulichkeit gilt nämlich nur für den Fall,

37 So z.B. das Business Practice Office (BPO) der Daimler AG; <https://Daimler.com/konzern/corporate-governance/compliance/bpo.html>; ähnlich die Abgrenzung bei der Allianz Deutschland AG, vgl. <http://allianz.de/compliance/>.

38 Baur/Holle, AG 2017, 379, 382.

39 So z.B. bei der Allianz Deutschland AG (siehe Fn. 38).

40 Vgl. § 25a Abs. 1 S. 6 Nr. 3 KWG.

dass die Hinweise berechtigt sind oder in gutem Glauben gegeben wurden.⁴¹ Die Schutzempfehlung des Kodex ändert daran nichts.

Fraglich ist weiter, ob der vom Kodex verlangte Schutz auch den Fall umfasst, dass ein Mitarbeiter tatsächliche oder vermeintliche Rechtsverstöße im Unternehmen bei externen Stellen wie z.B. der Staatsanwaltschaft anzeigt oder öffentlich macht. Ein solches Vorgehen verstößt im Allgemeinen gegen die arbeitsvertragliche Treue- und Verschwiegenheitspflicht des Mitarbeiters⁴² und kann dementsprechend arbeitsrechtliche Sanktionen nach sich ziehen. Soll ein *Whistleblower* auch in diesen Fällen geschützt sein? Dies erscheint zweifelhaft. Die Empfehlung gemäß Ziff. 4.1.3 S. 3 DCGK steht in unmittelbarem Zusammenhang mit der Erwähnung des Compliance-Management-Systems in Satz 1 dieser Ziffer. Dies spricht dafür, die Empfehlung allein auf das sog. interne *Whistleblowing* zu beziehen. Auch nach den erwähnten aufsichtsrechtlichen Bestimmungen, die der Kodex-Kommission vermutlich als Vorbild gedient haben, geht es allein um Meldungen an geeignete Stellen innerhalb des Unternehmens.⁴³ Daher ist anzunehmen, dass der vom Kodex verlangte Schutz nicht gilt, wenn Rechtsverstöße im Unternehmen gegenüber Stellen und Personen außerhalb des Unternehmens angezeigt werden.

Um den Schutz von Hinweisgebern, insbesondere bei Anzeigen an externe Stellen oder einem Gang an die Öffentlichkeit, zu verbessern, wird schon seit längerem über eine gesetzliche Regelung diskutiert. Dabei geht es vor allem um eine Ausweitung des Benachteiligungsverbotens gemäß § 612a BGB, das bislang nur Benachteiligungen auf Grund einer zulässigen Rechtsausübung untersagt.⁴⁴ Neben einer gesetzlichen Regelung zum internen *Whistleblowing* wurden auch Regelungen vorgeschlagen, wonach den Mitarbeitern generell oder unter bestimmten Voraussetzungen ein Anzeigerecht gegenüber externen Stellen zustehen soll.⁴⁵ Es liegt auf der Hand, dass ein solches Anzeigerecht das Vertrauensverhältnis zwischen Arbeitgeber und Arbeitnehmer erheblich beeinträchtigen kann.⁴⁶ Deshalb sind bislang alle diesbezüglichen Gesetzesvorschläge gescheitert. Der Umstand, dass die Kodex-Empfehlung diesen Bereich ausspart, könnte allerdings dazu führen, dass erneut der Ruf nach dem Gesetzgeber laut wird. Die Empfehlung in Ziff. 4. 1. 3. S. 3 DCGK erleidet dann möglicherweise dasselbe Schicksal wie andere Empfehlungen, die letzt-

41 *Baur/Holle*, AG 2017, 379, 381.

42 Vgl. § 241 Abs. 2 BGB und § 17 UWG.

43 Vgl. § 25a Abs. 1 S. 6 Nr. 3 KWG.

44 Vgl. den Entwurf eines Hinweisgeberschutzgesetzes der SPD-Fraktion vom 7. 2. 2012, BT-Drs. 17/8567 nebst der Kritik von *Mengel*, CCZ 2012, 146, sowie den Entwurf eines Whistleblower-Schutzgesetzes der Fraktion Bündnis 90/Die Grünen vom 4. 11. 2014, BT-Drs. 18/3039, sowie dazu die Beratungen im Ausschuss für Arbeit und Soziales, BT-Drs. 18/5148.

45 Vgl. die in vorstehender Fußnote erwähnten Gesetzesinitiativen.

46 Zu den in der Rechtsprechung behandelten Fällen *Reinhardt*, CB 2015, 299.

lich nur der Vorbereitung einer weiteren gesetzlichen Regulierung gedient haben.

4. Schutz beschuldigter Personen

Vom Kodex überhaupt nicht in den Blick genommen werden die Personen, die aufgrund eines Mitarbeiterhinweises dem Anfangsverdacht eines Rechtsverstoßes ausgesetzt sind. Auch diese Personen verdienen Schutz. Sie müssen aufgrund ihres allgemeinen Persönlichkeitsrechts zumindest die Möglichkeit haben, sich gegen wahrheitswidrige Anschuldigungen zu verteidigen. Dies ist bei anonymen Meldungen praktisch ausgeschlossen. Deshalb erscheint es angebracht, Hinweisgeber nur in der Weise zu schützen, dass ihnen die Vertraulichkeit ihrer Personalien zugesichert wird. Dies erlaubt den zuständigen Compliance-Stellen Rückfragen beim Hinweisgeber, durch welche die Aufklärungs- und Verteidigungsinteressen eines Beschuldigten gewahrt und eventuelle Falschbeschuldigungen aufgedeckt werden können.⁴⁷

5. Datenschutzrechtliche Anforderungen

Schließlich stellt sich die Frage, welche Anforderungen das Datenschutzrecht an ein Hinweisgebersystem stellt und ob die Empfehlung des DCGK damit vereinbar ist. Trotz wiederholter rechtspolitischer Forderung wurde bislang keine spezielle datenschutzrechtliche Regelung solcher Systeme geschaffen.⁴⁸

a) Gegenwärtige Rechtslage

Bei der Meldung von Regelverletzungen werden zumeist personenbezogene Daten erhoben, übermittelt und gespeichert. Davon betroffen sind sowohl die beschuldigte Person als auch der Hinweisgeber, dieser jedenfalls bei offenem Hinweis. Die Anforderungen, die das Datenschutzrecht an den Umgang mit personenbezogenen Daten stellt, sind vielfältig. So ist die Erhebung, Verarbeitung und Nutzung solcher Daten nur zulässig, wenn das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet, § 4a BDSG. Bei der konkreten Ausgestaltung eines Meldeverfahrens sind zudem weitere Vorgaben wie die Wahrung der Rechte des Betroffenen zu beachten.

Die rechtskonforme Einführung einer unternehmensinternen *Whistleblowing-Hotline* wird zwar durch die Empfehlungen der Aufsichtsbehörden⁴⁹

47 Casper, Liber Amicorum Winter, 2011, S. 77, 88, 92; vgl. auch Mahbold, NZA 2008, 737f.

48 Kort, MMR 2011, 294, 296 f.

49 Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz“ des Düsseldorfer Kreises: Whistleblowing Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, 2007, abrufbar unter https://www.datenschutz.hessen.de/download.php?download_ID=246.

und der Artikel-29-Datenschutzgruppe auf der Ebene der EU⁵⁰ erleichtert. Diese Vorschläge beruhen aber noch auf § 28 Abs. 1 S. 1 Nr. 2 BDSG a.F. Nach der Einfügung des § 32 BDSG zum Datenschutz der Beschäftigten bedarf die Rechtslage einer genaueren Betrachtung.

Zu unterscheiden sind zunächst Hinweise zur Aufdeckung von Straftaten und solche zur Verfolgung sonstiger Regelverletzungen, etwa Verstößen gegen Ethikrichtlinien.⁵¹ Bei den erstgenannten Hinweisen greift § 32 Abs. 1 S. 2 BDSG mit der Folge, dass ein dokumentierter, auf tatsächlichen Anhaltspunkten begründeter Verdacht einer Straftat vorliegen muss. Im Übrigen ist das Verhältnis von § 32 BDSG zu § 28 BDSG umstritten.⁵² Da mit der Einfügung des § 32 BDSG die materielle Rechtslage nicht verändert werden sollte,⁵³ kann § 32 Abs. 1 S. 2 BDSG jedenfalls keine Sperrwirkung dahin entnommen werden, dass Hinweisgeber-Systeme nur noch zur Verfolgung von Straftaten zulässig sein sollen.⁵⁴ Für die Abgrenzung des § 32 Abs. 1 S. 1 BDSG von dem nach wohl überwiegender Ansicht parallel anwendbaren⁵⁵ § 28 Abs. 1 S. 1 Nr. 2 BDSG ist ferner entscheidend, ob mit dem Hinweis eine Pflicht aus dem Arbeitsvertrag erfüllt wird.⁵⁶ Dies wird, wie bereits gezeigt, allenfalls bei schwerwiegenden Straftaten mit erheblichen Folgen für das Unternehmen, nicht jedoch bei Verstößen gegen Ethikrichtlinien der Fall sein.⁵⁷

Da beide Normen letztlich eine Interessenabwägung im Einzelfall verlangen, sollte ihre Anwendung im Regelfall zu demselben Ergebnis führen.⁵⁸ Die zentralen Vorgaben der Aufsichtsbehörden können damit unabhängig von der nunmehr einschlägigen Rechtsgrundlage auch weiterhin herangezogen werden. Die datenschutzgerechte Ausgestaltung eines Hinweisgebersystems muss demnach im Wesentlichen folgende Anforderungen erfüllen.⁵⁹

50 Artikel-29-Datenschutzgruppe: Stellungnahme 1/2006; abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_de.pdf.

51 Wolff/Brink/Riesenhuber, Datenschutzrecht in Bund und Ländern, 2013, § 32 BDSG Rdn. 115.

52 Vgl. nur Däubler/Klebe/Wedde/Weichert/Däubler, BDSG, 5. Aufl. 2016, § 32 BDSG Rdn. 8 ff.; Plath/Stamer/Kuhnke, BDSG/DSGVO, 2. Aufl. 2016, § 32 BDSG Rdn. 8 ff.; Auernhammer/Forst, DSGVO BDSG, 5. Aufl. 2017, § 32 BDSG Rdn. 13 ff.; Simitis/Seifert, BDSG, 8. Aufl. 2014, § 32 BDSG Rdn. 17.

53 BT-Drs. 16/13657, S. 21.

54 Forgó/Helfrich/Schneider/Schröder, Betrieblicher Datenschutz, 2. Aufl. 2017, Kap. 3, Rdn. 57; a.A. Haußmann/Kaufmann, ArbRAktuell 2011, 186, 187; Gola/Schomerus, BDSG, 12. Aufl. 2015, § 32 BDSG Rdn. 21.

55 Auernhammer/Kramer (Fn. 52), § 28 BDSG Rdn. 60 m.w.N.; Wolff/Brink/Wolff (Fn. 51), § 28 BDSG Rdn. 3.

56 Auernhammer/Kramer (Fn. 52), § 32 BDSG Rdn. 40.

57 Wisskirchen/Körber/Bissels, BB 2006, 1567, 1568.

58 Auernhammer/Forst (Fn. 52), § 32 BDSG Rdn. 16.

59 Vgl. Fn. 49.

- Die personenbezogenen Daten müssen für festgelegte eindeutige Zwecke erhoben und dürfen nicht in einer damit nicht zu vereinbarenden Weise weiterverarbeitet oder genutzt werden.⁶⁰
 - Im Rahmen einer Verhältnismäßigkeitsprüfung muss das Interesse an der Datenverarbeitung mit den Rechten des Betroffenen abgewogen werden.⁶¹ Bei der Meldung von sich gegen das Unternehmensinteresse richtenden Straftaten und Verhaltensweisen, die gegen Menschenrechte oder Umweltschutzbelange verstoßen, wird die Interessensabwägung in der Regel zugunsten des Unternehmens ausfallen. Bei Verletzung von Ethikrichtlinien überwiegen grundsätzlich die Interessen des Betroffenen.
 - Die Zahl der für die Meldung in Betracht kommenden Personen sowie der zu meldenden Personen ist möglichst zu begrenzen.
 - Hinweisgeber sollen ermutigt werden, nicht anonym, sondern unter Angabe ihres Namens zu handeln. Dabei ist sicher zu stellen, dass die Identität des Hinweisgebers vertraulich behandelt wird. Es sollte jedoch klargestellt werden, dass diese im Falle weitergehender Untersuchungen und Gerichtsverfahren den damit betrauten Personen bekannt werden kann.
 - Betroffenenrechte wie die Information der beschuldigten Person (§ 33 BDSG) sind zu wahren.
 - Daten sind spätestens innerhalb von zwei Monaten nach Abschluss der Untersuchung zu löschen (§ 35 BDSG).
- Die oben unter 2. bis 4. angestellten Überlegungen zum Gegenstand von Hinweisen und dem Schutz der Betroffenen haben damit auch eine datenschutzrechtliche Grundlage. Da die Vorschläge der Aufsichtsbehörden zum Datenschutz zwingendes Recht konkretisieren, sind diese auch bei der Auslegung und Umsetzung der Empfehlung in Ziff. 4. 1. 3 S. 3 DCGK zu berücksichtigen. Dies bedeutet im Einzelnen:
- Die weite Formulierung „Rechtsverstöße“ muss angesichts der vorzunehmenden Interessenabwägung teleologisch dahin eingeschränkt werden, dass nur solche Verstöße gemeint sind, die im Einzelfall ein überwiegendes Unternehmensinteresse begründen. Eine Beschränkung des Meldegegenstandes ist somit datenschutzrechtlich geboten.

60 Dies gilt unabhängig von der einschlägigen Rechtsgrundlage, da die in § 28 Abs. 1 S. 2 BDSG normierte Zweckbindung nach überwiegender Ansicht auch im Rahmen des § 32 BDSG zu beachten ist, vgl. Däubler/Klebe/Wedde/Weichert/Däubler (Fn. 52), § 32 BDSG Rdn. 9; Plath/Stamer/Kuhnke (Fn. 52), § 32 BDSG Rdn. 10; Thüsing, NZA 2009, 865, 866.

61 Dies gilt ebenfalls unabhängig von der einschlägigen Rechtsgrundlage, da dies einen der allgemeinen Grundsätze im Datenschutzrecht darstellt, welche nach der Gesetzesbegründung von der Einfügung des § 32 BDSG unberührt bleiben, vgl. BT-Drs. 16/13657, S. 21; Simitis/Seifert (Fn. 52), § 32 BDSG Rdn. 9; Plath/Stamer/Kuhnke (Fn. 52), § 32 BDSG Rdn. 16ff.

- Mit Blick auf die möglichst vorzunehmende Begrenzung des Personenkreises ist die Anregung, auch Dritten die Möglichkeit der Meldung zu gegeben, kritisch zu sehen.
- „Geschützt“ muss auch aus datenschutzrechtlicher Perspektive so ausgelegt werden, dass Meldungen offen und unter Zusicherung der Vertraulichkeit erfolgen sollen.

b) Geltendes Recht ab dem 25. 5. 2018

Auf die ab dem 25. 5. 2018 geltende Rechtslage sind diese Ergebnisse indes nicht ohne Weiteres übertragbar. Von diesem Zeitpunkt an bestimmen sich die datenschutzrechtlichen Anforderungen nämlich nach der Datenschutz-Grundverordnung (DS-GVO) und dem neuen BDSG.⁶²

Als Rechtsgrundlage kommen dann Art. 6 Abs. 1 lit. f) DS-GVO und § 26 Abs. 1 BDSG n.F. in Betracht.⁶³ Diese Normen stimmen im Wortlaut weitgehend mit § 28 Abs. 1 S. 1 Nr. 2 BDSG bzw. § 32 Abs. 1 BDSG überein.⁶⁴ Die bisherigen Unterscheidungskriterien sind daher im Grundsatz weiterhin anwendbar,⁶⁵ wenngleich eine unreflektierte Übertragung der Erkenntnisse zu § 28 BDSG aufgrund des Geltungsanspruchs der DS-GVO zu vermeiden ist.⁶⁶ Im Übrigen sind die aufgezeigten Vorgaben zwar teilweise in der DS-GVO wiederzufinden, etwa die Grundsätze der Zweckbindung und Datenminimierung in Art. 5 Abs. 1 lit. b) und c) DS-GVO. Die neue Rechtslage bringt jedoch einige zusätzliche Anforderungen mit sich. Insbesondere wird das Auskunftsrecht des Betroffenen durch Art. 15 DS-GVO deutlich ausgeweitet.⁶⁷ Zudem ist die Transparenz der Datenverarbeitung im Rahmen der Interessenabwägung stärker zu berücksichtigen und eine engere Abstimmung mit dem Datenschutzbeauftragten erforderlich.⁶⁸ Die Gesellschaften stehen daher vor der Aufgabe, ihre Hinweisgeber-Systeme nach den veränderten Anforderungen zu gestalten. Zur Absicherung dieser Ausgestaltung wäre, auch angesichts der erheblich verschärften Sanktionen (vgl. Art. 83 DS-GVO), eine Aktualisierung der bisherigen aufsichtsrechtlichen Vorgaben zu begrüßen.

IV. Schlussbemerkung

Die Empfehlung des Kodex an alle börsennotierten Gesellschaften, ein Hinweisgebersystem einzurichten, folgt der allgemeinen Tendenz, den Bereich Compliance durch immer neue organisatorische Vorgaben auszubauen.

62 Vgl. z.B. Paal/Pauly, DS-GVO, 2017, Einleitung Rdn. 1 ff.

63 Forgó/Helfrich/Schneider/Schröder (Fn. 54), Kap. 3, Rdn. 57.

64 Zu § 26 BDSG vgl. BT-Drs. 18/11325, S. 96 f.

65 Vgl. Forgó/Helfrich/Schneider/Schröder (Fn. 54), Kap. 3, Rdn. 57.

66 Vgl. Paal/Pauly/Frenzel (Fn. 62), Art. 6 Rdn. 52.

67 Paal/Pauly/Paal (Fn. 62), Art. 15 Rdn. 45; Müller/Janicki, InTeR 2016, 213, 214.

68 Wybitul, CCZ 2016, 194, 195 f.

Die Einrichtung eines solchen Systems ist jedoch allenfalls bei großen Unternehmen angebracht, die ein derartiges System zumeist schon haben. Unabhängig davon lässt die Empfehlung des Kodex viele Fragen offen. Dies ist einerseits zu begrüßen, weil sie den Vorständen einen weiten Spielraum bei der Umsetzung der Empfehlung einräumt. Andererseits lässt die gewählte Formulierung die datenschutzrechtlichen Anforderungen unberücksichtigt. Wichtige Rechtsfragen, insbesondere zum Schutz des Hinweisgebers und etwaiger Beschuldiger, bleiben ungeklärt. Eine präzisere Formulierung wäre angesichts der notwendigen korrigierenden Auslegung wünschenswert. Nach den bisherigen Erfahrungen sollte es daher nicht überraschen, wenn die Kodex-Empfehlung in den kommenden Jahren weiter verfeinert oder durch gesetzliche Regelungen ersetzt wird.

Reinhard Marsch-Barner