

IT-Compliance an Hochschulen

Bearbeitet von
Dr. Ingo Schöttler

1. Auflage 2010. Taschenbuch. 240 S. Paperback
ISBN 978 3 415 04465 4
Format (B x L): 14,5 x 20,8 cm

[Weitere Fachgebiete > Pädagogik, Schulbuch, Sozialarbeit > Schulen, Schulleitung > Universitäten, Hochschulen](#)

Zu [Inhaltsverzeichnis](#)

schnell und portofrei erhältlich bei


DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

2. Kapitel

Der Begriff der IT-Compliance

A. IT-Compliance als rechtliche Kategorie

Um sinnvolle Aussagen über IT-Compliance-Konzepte für beziehungsweise an Hochschulen treffen zu können, ist zunächst zu bestimmen, was unter dem Begriff der „IT-Compliance“ genau zu verstehen ist. Erst im Anschluss an diese Begriffsklärung kann dann untersucht werden, inwieweit IT-Compliance auch für Hochschulen von Bedeutung ist, und welche Bestandteile derartige Konzepte enthalten sollten.

I. Der Begriff der „Compliance“

Bevor auf den Sonderbereich der IT-Compliance eingegangen werden kann, sollte der Begriff zunächst in seiner allgemeinen Bedeutung bestimmt werden.

Der Begriff „Compliance“ bedeutet in direkter wörtlicher Übersetzung aus dem Englischen soviel wie „Wohlverhalten“ oder „Befolgung“.⁵ In rechtlicher Hinsicht versteht man unter dem Begriff vielfach ein Handeln in Übereinstimmung mit dem Gesetz beziehungsweise mit den jeweils einschlägigen Regelungen.⁶ Im Hinblick auf eine derartige „enge“ Definition des „Compliance“-Begriffes ist allerdings zu Recht angemerkt worden, dass es für Unternehmen und andere Organisationen eine schlichte Selbstverständlichkeit ist, dass diese die für sie einschlägigen gesetzlichen Regelungen befolgen müssen.⁷ Es würde sich hierbei dann um kein neuartiges Konzept handeln, das zunächst aus dem anglo-amerikanischen Rechtsraum nach Deutschland importiert werden musste.⁸

Um den Begriff sinnvoll verwenden zu können, ohne damit bloße Selbstverständlichkeiten auszudrücken, bietet sich daher eine „weitere“ Definition des Begriffes an: Verstanden werden sollte „Compliance“ nicht nur als Einhaltung der für eine Organisation geltenden Regelungen, sondern vielmehr darüber hinaus als Bezeichnung für den Aufbau einer Organisationsstruktur mit einem entsprechenden Risikomanagement, das die Einhaltung der jeweils anwendbaren gesetzlichen Regelungen weitestgehend

5 Vgl. hierzu und zu weiteren möglichen Übersetzungen des Wortes „compliance“ zum Beispiel das Internetwörterbuch „LEO“, abrufbar unter: <http://www.leo.org/>.

6 Lösler, NZG 2005, 104, 104; Münch in: Taeger/Rath, IT-Compliance als Risikomanagement-Instrument, S. 92; Welp in: Taeger/Rath, IT-Compliance als Risikomanagement-Instrument, S. 79.

7 Schneider, ZIP 2003, 645, 646.

8 Siehe hierzu sogleich *Gliederungspunkt A. 2.*

garantieren kann.⁹ „Compliance“ bedeutet danach nicht nur die geltenden Regelungen einzuhalten, sondern vielmehr beschäftigen sich entsprechende Compliance-Konzepte mit den Wegen und Möglichkeiten, wie dies in einer Organisationsstruktur erreicht werden kann. Die Maßnahmen, die hierzu vornehmlich in den USA entwickelt wurden, waren tatsächlich vor der „Einführung“ des Begriffs in Deutschland vielfach noch nicht bekannt beziehungsweise sie wurden nicht von einer größeren Anzahl von Unternehmen umgesetzt.¹⁰ Wenn man daher den Begriff „Compliance“ mit diesem weiten Sinngehalt verwendet, handelt es sich nicht lediglich um einen überflüssigen „Mode-Begriff“, unter dem juristische Selbstverständlichkeiten präsentiert werden.

II. Die Entwicklung des Begriffes

Entwickelt wurden moderne „Compliance“-Methoden zunächst vornehmlich in den USA.¹¹ Es lässt sich naturgemäß nur schwer festlegen, zu welchem Zeitpunkt genau die Entwicklung von Compliance-Programmen begann. Als ein wichtiger Ausgangspunkt für moderne Compliance-Konzepte kann jedoch der Erlass der so genannten „Federal Sentencing Guidelines“ (FSG) gelten, deren Ziel die Eindämmung der Wirtschaftskriminalität ist.¹² Durch die FSG wird Richtern in den USA seit 1991 die Möglichkeit eröffnet, ein Urteil gegen Unternehmen bei Vorliegen bestimmter Umstände abzumildern. Zu diesen Umständen zählt auch die Existenz eines unternehmensinternen Compliance-Systems, um Rechtsverstöße zu verhindern.¹³ Die FSG bildeten daher für viele Unternehmen ein starkes Motiv, um umfassende Compliance-Systeme zu entwickeln und umzusetzen.

Kurze Zeit nachdem sich entsprechende Compliance-Programme in den USA etabliert hatten, hielt der Begriff auch Einzug in den deutschen Sprach- und Rechtsraum, ohne dass ein nennenswerter Versuch bekannt

9 Vgl. Hauschka, NJW 2004, 257, 257; ähnlich auch *Rath* in: Taeger/Rath, IT-Compliance als Risikomanagement-Instrument, S. 5.

10 Vgl. Schneider, ZIP 2003, 645, 645, der darauf hinweist, dass amerikanische Unternehmen spätestens mit Beginn der 90er Jahre des vergangenen Jahrhunderts Compliance-Programme eingeführt haben.

11 Schneider, ZIP 2003, 645, 645.

12 Bürkle, BB 2005, 565, 565.

13 Erforderlich ist in diesem Zusammenhang, dass das Unternehmen über ein „effective program to prevent and detect violations of law“ verfügt; vgl. hierzu Bergmoser/Theusinger/Gushurst, BB-Spezial 5.2008 zu Heft 25, 1, 2; neben diese Regelungen sind inzwischen weitere entsprechende Regelungen getreten, die im Jahre 2002 durch den Sarbanes-Oxley Act (SOX) eingeführt wurden; hiernach wird von Unternehmen die Errichtung eines umfassenden internen Kontrollsystems verlangt, vgl. hierzu Bergmoser/Theusinger/Gushurst, BB-Spezial 5.2008, 1, 3.

ist, den Begriff ins Deutsche zu übersetzen.¹⁴ Hierbei ist zu berücksichtigen, dass der Versuch einer derartigen Übersetzung auch zu neuen Missverständnissen führen könnte. Denn wörtliche Übersetzungen des Begriffes wie „Wohlverhalten“ oder „Befolgung“ würden wiederum ein eher „enges“ Verständnis des Begriffs nahe legen, das jedoch wenig sinnvoll ist.

Zunächst wurde der „Compliance“-Begriff in Deutschland fast ausschließlich in Bezug auf die Einhaltung ganz bestimmter Rechtsnormen verwendet. Gebräuchlich war der Begriff in Zusammenhang mit den Vorgaben des Wertpapierhandelsgesetzes oder des Kartellrechts.¹⁵ Im Laufe der Zeit setzte sich jedoch ein „weiterer“ Compliance-Begriff durch. Compliance-Maßnahmen können sich nach dem heutigen Verständnis auf alle Bereiche eines Unternehmens und auch auf alle Rechtsgebiete beziehen. Compliance kann daher nunmehr auch im deutschen Rechts- und Sprachraum definiert werden als die Gesamtheit aller organisatorischen Maßnahmen, die zum Ziel haben, dass sich ein Unternehmen beziehungsweise dessen Mitarbeiter (vollumfänglich) rechtskonform verhalten.¹⁶ Ausgehend von diesem weiten Compliance-Verständnis haben sich dann auch Unterkategorien herausgebildet, die Maßnahmen in Bezug auf ganz bestimmte Rechtsgebiete und Unternehmensgebiete beinhalten. Zu diesen Unterkategorien gehört auch der Bereich der IT-Compliance.

III. Die Ziele und der Zweck einer Compliance

1. Sicherstellung rechtskonformen Verhaltens

Wie bereits aufgezeigt, ist das primäre Ziel von Compliance-Maßnahmen zu erreichen, dass ein Unternehmen beziehungsweise dessen Mitarbeiter die geltenden rechtlichen Regelungen einhalten. Um dieses Ziel zu erreichen, dienen Compliance-Maßnahmen dabei mehreren „Unterzielen“: Zunächst sollen sie präventiv bewirken, dass es im Bereich des Unternehmens überhaupt nicht zu Verhaltensweisen kommt, die einen Verstoß gegen einschlägige Vorgaben bedeuten können. Dieser präventive Zweck kann vornehmlich durch eine umfassende Information der Mitarbeiter und die Vorgabe

14 Lösler, NZG 2005, 104, 104; zur Kritik an diesem „Denglisch“ in der Rechtssprache vgl. auch Hauschka, ZRP 2006, 258 ff.

15 Vgl. Mengel, BB 2006, 2466, 2467.

16 Vgl. Bürkle, BB 2005, 565, 565; Schneider, ZIP 2003, 645, 646; *Rath* in: Taeger/Rath, IT-Compliance als Risikomanagement-Instrument, S. 5; diesem erweiterten Verständnis folgt nun auch der „Deutsche Corporate Governance Kodex“, ein von der „Regierungskommission Deutscher Corporate Governance Kodex“ entwickelter „Code of Best Practice für Unternehmen“, in dem unter Ziffer 4.31. ausgeführt wird: „Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).“.

bestimmter Verhaltensregeln sowie die Androhung von Sanktionen bei Verstößen verwirklicht werden.¹⁷

Neben diesem Ziel der Verhinderung von möglichen Rechtsverstößen beziehungsweise der Vermeidung von kritischen Verhaltensweisen ist ein weiteres Ziel von Compliance-Maßnahmen, bestehende problematische Strukturen aufzudecken, die zu einem Rechtsverstoß führen könnten oder bereits einen Rechtsverstoß darstellen.¹⁸ Werden sie erkannt, können derartige Verhaltensweisen dann abgestellt werden, bevor sie für das betroffene Unternehmen weitergehende negative Konsequenzen haben.

In diesem Zusammenhang ist auch zu berücksichtigen, dass die Einhaltung der einschlägigen rechtlichen Regelungen im Regelfall nicht idealistischer Selbstzweck sein wird, sondern dass die Unternehmensleitung mit der Durchführung derartiger Compliance-Maßnahmen normalerweise darüber hinausgehende beziehungsweise daran anschließende Ziele verfolgt:

2. Schadensprävention

An erster Stelle ist die Schadensprävention zu nennen.¹⁹ Ein Verstoß gegen Rechtsnormen kann für Unternehmen sowohl zivilrechtliche als auch öffentlich-rechtliche und für die betroffenen Mitarbeiter auch strafrechtliche Konsequenzen nach sich ziehen.²⁰ In einigen Rechtsbereichen sind inzwischen Geldbußen in einer Größenordnung vorgesehen, die auch Großunternehmen empfindlich treffen können. Dies gilt insbesondere für den Bereich des Kartellrechts. So hat zum Beispiel die EU-Kommission gegen den Siemens-Konzern im Januar 2007 einen Bußgeldbescheid über insgesamt 418 Millionen Euro wegen Verstößen gegen kartellrechtliche Rechtsnormen erlassen.²¹

Hierbei ist zu beachten, dass das Risiko einer Haftung für Unternehmen im zivilrechtlichen Bereich durch verschiedene gesellschaftliche Entwicklungen der letzten Jahre gestiegen ist. So können sich sowohl Konsumenten als auch Kleinunternehmer mit Hilfe der modernen Kommunikationsmedien, zu denen auch das Internet zählt, heute in einem viel größeren Umfang über bestimmte Unternehmen informieren, als dies noch vor ein paar Jahren der Fall war. Mögliche Rechtsverstöße oder Unregelmäßigkeiten innerhalb eines Unternehmens werden damit einhergehend auch viel

17 Lampert, BB 2002, 2237, 2239.

18 Lampert, BB 2002, 2237, 2239.

19 Bürkle, BB 2005, 565, 566.

20 Vgl. zu den möglichen Rechtsfolgen noch eingehend *Kapitel 5*.

21 Vgl. den entsprechenden Bericht bei SPIEGEL ONLINE, abrufbar unter: <http://www.spiegel.de/wirtschaft/0,1518,461907,00.html>; Siemens kündigte an, gegen diesen Bescheid vor dem Europäischen Gerichtshof zu klagen.

schneller in der breiten Öffentlichkeit publik.²² Hierdurch steigt das Risiko entsprechender Klagen von Kunden oder von Kleinaktionären. Zu dieser Entwicklung trägt weiter bei, dass inzwischen spezialisierte Anwaltskanzleien – auch in Deutschland – am Markt tätig sind, die auf die Durchführung entsprechender Sammelklagen und Verfahren spezialisiert sind.²³

3. Haftungsreduzierung der Unternehmensleitung

Weiterhin sollen Compliance-Programme vielfach dazu dienen, die Haftung der Leitungsebene einer Organisation einzuschränken. Hierbei müssen zwei Gesichtspunkte getrennt betrachtet werden: Zum einen wird das Risiko der Haftung der Leitungsebene für Compliance-Verstöße dadurch minimiert, dass die Zahl von Rechtsverstößen im Unternehmen verringert wird. Zum anderen kann bereits der Nachweis der Unternehmensleitung, bestimmte Compliance-Programme durchgeführt zu haben, ausreichend sein, um eine Haftung zu vermeiden.²⁴ In diesem Zusammenhang ist festzustellen, dass insbesondere die Haftung von Aufsichtsräten von Aktiengesellschaften in den letzten Jahren ausgeweitet wurde. Ursächlich hierfür war die Einführung neuer gesetzlicher Regelungen wie das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), aber auch eine Erweiterung der Haftung durch die Rechtsprechung, insbesondere durch die „ARAG/Garmenbeck“-Entscheidung des BGH.²⁵ Hiernach besteht eine Verpflichtung des Aufsichtsrats zur Geltendmachung von Ansprüchen der Gesellschaft gegenüber den Vorständen, falls dies nach sachgerechter Prüfung Erfolg versprechend erscheint.²⁶ Neben dieser Haftung kann eine Verletzung von Aufsichtspflichten auch eine Verletzung des entsprechenden Dienstvertrages bedeuten, und unter Umständen auch eine fristlose Kündigung eines Vorstandsmitglieds rechtfertigen.²⁷ Diese erhöhten Haftungsrisiken führen in der Praxis vielfach dazu, dass der Durchführung von Compliance-Programmen in Unternehmen inzwischen eine große Aufmerksamkeit zukommt.

4. Vermeidung von Ansehensverlusten

Weiterhin geht es neben der Vermeidung von direkten materiellen Schäden, die derartige Rechtsverstöße für Unternehmen bedeuten können, vielfach auch darum, einen Ansehensverlust zu vermeiden. Dieser kann bei der öffentlichen Aufdeckung von Rechtsverstößen zunächst bei den jeweiligen

²² Im Internet formiert sich zunehmend eine Gruppe von politisch interessierten Nutzern mit einer Art „Global citizenship“, vgl. Busse, DIE ZEIT/INTERNET SPEZIAL, Mai 2008, S. 28.

²³ Hauschka, NJW 2004, 257, 258.

²⁴ Siehe hierzu noch unten *Gliederungspunkt A. IV.*

²⁵ BGH, NJW 1997, 1926; vgl. auch den entsprechenden Nachweis bei Hauschka, NJW 2004, 257, 257.

²⁶ BGH, NJW 1997, 1926, 1928.

²⁷ Vgl. LG Berlin, AG 2002, 682.

Kunden auftreten, wenn ein häufig über Jahre aufgebautes „sauberes“ Image durch illegales Handeln zerstört wird. Ein derartiger Ansehensverlust kann sich dann auch auf die Umsätze eines Unternehmens und seine Marktanteile auswirken. Neben diesen Kundenreaktionen können derartige Negativmeldungen auch Auswirkungen auf das Verhalten der Stakeholder des Unternehmens haben, was insbesondere bei börsennotierten Gesellschaften eine negative Entwicklung des Aktienkurses zur Folge haben kann.²⁸

IV. Compliance-Programme als rechtliche Notwendigkeit?

Vor diesem Hintergrund ist es für Unternehmen in mehrfacher Hinsicht sinnvoll und ratsam, Compliance-Maßnahmen durchzuführen. Die weitergehende Frage, die sich hieran anschließt, ist jedoch, inwieweit nach der bestehenden Rechtslage bestimmte Compliance-Maßnahmen nicht nur empfehlenswert, sondern vielmehr gesetzlich vorgeschrieben sind.

Hierbei ist wiederum zu berücksichtigen, dass der Compliance-Begriff in seiner vorzuziehenden weiten Auslegung mehr einschließt als die bloße Einhaltung der gesetzlichen Vorgaben.²⁹ Zur Einhaltung dieser Vorgaben sind alle Unternehmen selbstverständlich verpflichtet.³⁰ Fraglich ist jedoch, inwieweit die Verpflichtung besteht Konzepte umzusetzen, um die Einhaltung dieser Regelungen weitgehend zu garantieren.

1. Die Vorgaben des Aktiengesetzes

Eine solche rechtliche Notwendigkeit der Durchführung von Compliance-Maßnahmen kann sich aus § 91 Abs. 2 AktG ergeben.³¹ Hiernach ist der Vorstand einer Aktiengesellschaft gesetzlich verpflichtet, die geeigneten Maßnahmen zu treffen und ein Überwachungssystem einzurichten, um solche Entwicklungen innerhalb des Unternehmens früh genug zu erkennen, die den Fortbestand der Gesellschaft gefährden können. Wenn Vorstandsmitglieder gegen diese sich aus § 91 Abs. 2 AktG ergebenden Verpflichtungen verstoßen, droht ihnen ein Schadensersatzanspruch aus § 93 Abs. 2 AktG.³² Danach sind Vorstandsmitglieder, die ihre Pflichten verletzen, der Gesellschaft zum Ersatz des daraus entstehenden Schadens verpflichtet. Die Vorschrift des § 91 Abs. 2 AktG wurde 1998 durch das KonTraG³³ in

28 Bürkle, BB 2005, 565, 566.

29 Siehe hierzu bereits oben unter *Gliederungspunkt A. II.*

30 Hierzu siehe bereits oben unter *Gliederungspunkt A. I.*

31 § 91 Abs. 2 AktG lautet:

„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“.

32 Vgl. Begr. RegE, BT-Drs. 13/9712, S. 15.

33 Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, BGBl. I 1998, 786.

das Aktiengesetz eingefügt. Compliance-Maßnahmen stellen insoweit ein Überwachungssystem dar, das dazu dient, ein rechtskonformes Verhalten aller Mitarbeiter eines Unternehmens zu erreichen. Weiterhin kann ein rechtswidriges Verhalten von Unternehmensmitarbeitern im Hinblick auf die damit zum Teil verbundenen erheblichen Rechtsfolgen durchaus den Fortbestand der Gesellschaft i. S. d. § 91 Abs. 2 AktG gefährden.³⁴ Auch die entsprechende Gesetzesbegründung nennt als Beispiele für gefährdende Maßnahmen i. S. d. § 91 Abs. 2 AktG unter anderem Verstöße gegen gesetzliche Regelungen, die sich auf die Vermögens-, Finanz- und Ertragslage der Gesellschaft oder des Konzerns wesentlich auswirken.³⁵ Hierbei ist zu berücksichtigen, dass bei Rechtsverletzungen neben der Verhängung von erheblichen Bußgeldern auch zunehmend zivilrechtliche Schadensersatzforderungen von geschädigten Dritten drohen.³⁶ Daher ist nach der Auslegung der Vorschrift davon auszugehen, dass durch § 91 Abs. 2 AktG zumindest in einem gewissen Umfang die Einrichtung von Compliance-Maßnahmen vorgeschrieben wird. Dabei gilt die Regelung nach allgemeiner Ansicht nicht nur für Aktiengesellschaften, sondern sinngemäß auch für GmbHs und andere Gesellschaftsformen.³⁷ Nach der Gesetzesbegründung soll die Norm Ausstrahlungswirkung auch auf den Pflichtenrahmen der Geschäftsführer anderer Gesellschaftsformen haben.³⁸ Auch diese trifft daher zumindest in einem gewissen Umfang die Pflicht zur Compliance, je nach der Größe und der Struktur der Gesellschaft.

Wie weitreichend allerdings die Anforderungen sind, die sich aus § 91 Abs. 2 AktG im Detail ergeben, ist in der Literatur umstritten: Teilweise wird aus der Regelung die Notwendigkeit abgeleitet, ein komplexes und umfangreiches Risikomanagementsystem für das Unternehmen aufzubauen.³⁹ Die wohl herrschende Meinung geht jedoch davon aus, dass durch § 91 Abs. 2 AktG nicht derartig weitgehende Verpflichtungen vorgeschrieben werden. Dem Vorstand werde nicht vorgegeben, ein umfassendes Risikomanagementsystem einzurichten, sondern er müsse lediglich ein Früherkennungssystem schaffen, mit dem akute, den Bestand der Gesellschaft gefährdende Risikolagen rechtzeitig identifiziert werden könnten.⁴⁰ Nach

34 Vgl. zu diesen teilweise erheblichen Rechtsfolgen bereits oben *Gliederungspunkt A. III. 2.*

35 Vgl. Begr. RegE, BT-Drs. 13/9712, S. 15.

36 Vgl. Fleischer, AG 2003, 291, 299.

37 *Lensdorf/Steger* in: Taeger/Wiebe, Aktuelle Rechtsfragen zu IT und Internet, S. 170; vgl. auch *Wecker* in: Taeger/Rath, IT-Compliance als Risikomanagement-Instrument, S. 33, der zu Recht darauf hinweist, dass es der Gesetzgeber allerdings unterlassen habe, eine § 91 Abs. 2 AktG entsprechende Regelung in das GmbHG aufzunehmen, so dass man nicht von gänzlich gleichlautenden Verpflichtungen ausgehen könne.

38 Vgl. Begr. RegE, BT-Drs. 13/9712, S. 15.

39 In diese Richtung argumentierend *Hauschka* in: Unmuß, Corporate Compliance Checklisten, S. X; vgl. auch die Nachweise bei Fleischer, AG 2003, 291, 298.

40 Fleischer, AG 2003, 291, 298; Bergmoser/Theusinger/Gushorst, BB-Spezial 5.2008, S. 1, 4.

der Gesetzesbegründung soll der Vorstand durch § 91 Abs. 2 AktG verpflichtet werden, für ein angemessenes Risikomanagement und eine angemessene interne Revision zu sorgen.⁴¹ Die entsprechenden Überwachungsmaßnahmen müssten so eingerichtet werden, dass problematische Entwicklungen frühzeitig, also zu einem Zeitpunkt erkannt würden, in dem noch geeignete Maßnahmen zur Sicherung des Fortbestands der Gesellschaft getroffen werden könnten.⁴²

Letztendlich lässt sich aus § 91 Abs. 2 AktG nicht entnehmen, welche Maßnahmen eine Gesellschaft im Einzelfall genau treffen muss, und wie umfangreich diese Maßnahmen ausgestaltet sein müssen. Dies ist entscheidend von der Größe und Struktur des Unternehmens abhängig und der Branche, in der es tätig ist.⁴³ Unstreitig ist jedoch, dass sich aus § 91 Abs. 2 AktG ergibt, dass der Vorstand eines Aktienunternehmens Compliance-Programme installieren muss, auch wenn dieser Begriff in der Norm selbst nicht verwendet wird.

2. Vorgaben aus § 130 OWiG

Zumindest indirekt wird die Pflicht zum Aufbau einer Compliance-Organisation auch aus § 130 OWiG hergeleitet.⁴⁴ Hiernach handelt der Inhaber eines Betriebes oder eines Unternehmens ordnungswidrig, wenn er vorsätzlich oder fahrlässig Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber als solchen treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre.

§ 130 OWiG verpflichtet den Betriebs- oder Unternehmensinhaber daher nicht direkt zur Durchführung von Compliance-Maßnahmen, droht jedoch eine Strafe oder Geldbuße an, wenn die beschriebenen Aufsichtsmaßnahmen, die ja eine Form von Compliance-Maßnahmen darstellen, unterlassen werden. So ist es zum Beispiel bei Kartellverstößen üblich, gegen die verantwortlichen Organmitglieder wegen einer Verletzung der Aufsichtspflicht gemäß § 130 OWiG zu ermitteln. Obwohl § 130 OWiG daher keine direkte Verpflichtung zu entnehmen ist, Compliance-Strukturen in einem Unternehmen umzusetzen, finden sich allerdings in der Rechtsprechung zu § 130 OWiG vereinzelte Vorgaben zu konkreten Maßnahmen, wie zum Beispiel die Einrichtung einer Revision oder anderer Institutionen.⁴⁵

41 Vgl. Begr. RegE, BT-Drs. 13/9712, S. 15.

42 Vgl. Begr. RegE, BT-Drs. 13/9712, S. 15.

43 Vgl. Begr. RegE, BT-Drs. 13/9712, S. 15; *Wecker* in: *Taeger/Rath, IT-Compliance als Risikomanagement-Instrument*, S. 23, 33.

44 Vgl. *Schneider*, ZIP 2003, 645, 649.

45 Vgl. die Nachweise bei *Hauschka*, ZIP 2004, 877, 878, aus dessen Sicht sich die Rechtsprechung in derartigen Fällen nur in „organisatorische[n] Ratschläge[n] verirrt“ habe.

3. Vorgaben in Spezialgesetzen

Weitere Vorgaben für den Aufbau einer Compliance-Organisation finden sich weiterhin in einer Vielzahl von spezialgesetzlichen Regelungen. Diesen Vorgaben ist gerade gemein, dass sie jeweils nicht für alle Unternehmen gelten, sondern nur für Unternehmen in einer speziellen Branche beziehungsweise einem speziellen Betätigungsfeld. Genannt werden können zum Beispiel die speziellen Vorgaben, die für Kreditinstitute gelten. Gemäß § 25a Abs. 1 S. 1 KWG muss ein entsprechendes Institut über eine ordnungsgemäße Geschäftsorganisation verfügen, die die Einhaltung der vom Institut zu beachtenden gesetzlichen Bestimmungen und der betriebswirtschaftlichen Notwendigkeiten gewährleistet. Ein Teil dieser ordnungsgemäßen Geschäftsorganisation ist gemäß § 25a Abs. 1 S. 3 KWG ein angemessenes und wirksames Risikomanagement.⁴⁶

Eine ähnliche Regelung existiert auch für Wertpapierdienstleistungsunternehmen. Hier ergibt sich aus § 33 Abs. 1 S. 1 WpHG die Verpflichtung, ebenfalls die organisatorischen Pflichten nach § 25 Abs. 1 und 4 KWG einzuhalten. Darüber hinaus werden in § 33 Abs. 1 WpHG noch weitere organisatorische Pflichten genannt. Hierzu gehört nach § 33 Abs. 1 Nr. 1 WpHG, angemessene Grundsätze aufzustellen, Mittel vorzuhalten und Verfahren einzurichten, die darauf ausgerichtet sind, sicherzustellen, dass das Wertpapierdienstleistungsunternehmen selbst und seine Mitarbeiter den Verpflichtungen dieses Gesetzes nachkommen, wobei eine dauerhafte und wirksame Compliance-Funktion einzurichten ist, die ihre Aufgaben unabhängig wahrnehmen kann. § 33 WpHG stellt damit auch eine der ersten Vorschriften dar, in denen der Begriff „Compliance“ ausdrücklich genannt wird.

Ein weiteres Beispiel für eine Norm, die entsprechende Organisationsstrukturen fordert, ist § 14 GeldwäscheG. Danach sind verschiedene Unternehmen (unter anderem Kreditinstitute und Finanzdienstleistungsinstitute) verpflichtet, Vorkehrungen dagegen zu treffen, dass sie zur Geldwäsche missbraucht werden. Zu diesen Vorkehrungen gehört gemäß § 14 Abs. 2 Nr. 2 GeldwäscheG die Entwicklung interner Grundsätze, angemessener geschäfts- und kundenbezogener Sicherungssysteme und Kontrollen zur Verhinderung der Geldwäsche und der Finanzierung terroristischer Vereinigungen. Der Begriff „Compliance“ wird in der Norm zwar nicht ausdrücklich genannt, aus der Vorschrift ergibt sich aber zumindest indirekt die Verpflichtung zur Installation entsprechender Compliance-Systeme, die ja gerade der Verhinderung illegalen Verhaltens dienen sollen.

⁴⁶ Die näheren Anforderungen an ein derartiges Risikomanagement werden in § 25a KWG noch näher beschrieben.

Die bisherigen Beispiele verdeutlichen, dass die gesetzliche Verpflichtung zum Aufbau von Compliance-Systemen bislang vielfach Unternehmen der Finanzbranche betrifft.

Auch Unternehmen in anderen Tätigkeitsfeldern können jedoch zur Durchführung von Compliance-Maßnahmen verpflichtet sein. So enthält beispielsweise § 52a BImSchG eine (indirekte) Verpflichtung zur Durchführung von Compliance-Maßnahmen.⁴⁷ Danach muss gemäß § 52 Abs. 2 BImSchG der Betreiber einer genehmigungsbedürftigen Anlage nach dem BImSchG der zuständigen Behörde mitteilen, auf welche Weise sichergestellt ist, dass die dem Schutz vor schädlichen Umwelteinwirkungen und vor sonstigen Gefahren, erheblichen Nachteilen und erheblichen Belästigungen dienenden Vorschriften und Anordnungen beim Betrieb beachtet werden. Mit anderen Worten: Es muss gerade nachgewiesen werden, dass entsprechende Compliance-Programme in diesem Bereich durchgeführt wurden.

4. Vorgaben für andere Organisationen

Wie bereits dargestellt, gelten die allgemeinen „Compliance-Vorgaben“, die sich aus § 91 Abs. 2 AktG ergeben, nicht nur für Aktiengesellschaften, sondern sinngemäß auch für andere Gesellschaften und deren Geschäftsführer. Von der Ausstrahlungswirkung des § 91 Abs. 2 AktG werden jedoch nicht alle Organisationen erfasst, bei denen der Aufbau eines Compliance-Systems sinnvoll wäre. Ausgespart hiervon bleiben alle öffentlich-rechtlichen Stellen, und somit grundsätzlich auch Hochschulen.⁴⁸

Aber auch für den privatrechtlichen Bereich wird bestritten, dass tatsächlich nach der geltenden Rechtslage für alle Unternehmen die Verpflichtung besteht, eine Compliance-Organisation einzurichten beziehungsweise aufzubauen.⁴⁹ Entsprechende konkrete organisatorische Vorgaben ließen sich allenfalls der Rechtsprechung zu § 130 OWiG entnehmen. Ansonsten müssten jedoch die Leitungsorgane eines Unternehmens entscheiden, ob sie sich selbst für befähigt hielten, die Rechtstreue eines Unternehmens zu gewährleisten, oder ob hierfür der Aufbau einer Compliance-Organisation notwendig sei.⁵⁰

47 Vgl. den entsprechenden Nachweis bei Schneider, ZIP 2003, 645, 649.

48 Siehe zu einer möglichen gesetzlichen Verpflichtung von Hochschulen beziehungsweise der Hochschulleitung zur Durchführung von Compliance-Maßnahmen *Kapitel 6*.

49 So Hauschka, ZIP 2004, 877, 878.

50 Hauschka, ZIP 2004, 877, 878.