

Haftung und Compliance: Wie beeinflusst eine CMS-Zertifizierung den Sorgfaltstaßstab?

Mona Philomena Ladler*, Universität Klagenfurt

Kurztext: Eine ungenügende Compliance-Organisation stellt eine Sorgfaltspflichtverletzung der Geschäftsleiter dar. CMS-Standards, wie die Norm ISO 19600, bieten Hilfestellungen zur Ausgestaltung einer Compliance-Organisation und können daher das Haftungsrisiko der Geschäftsleitung reduzieren. In diesem Beitrag wird der Frage nach der Rechtsqualität von CMS-Standards nachgegangen. Es werden die Haftungsfolgen einer Zertifizierung einer Compliance-Organisation auf Basis von CMS-Standards untersucht und analysiert, ob die ordentliche Sorgfalt die Errichtung einer den CMS-Standards entsprechenden Compliance-Organisation gebieten kann.

Schlagworte: ordentliche Sorgfalt; gewissenhafter Geschäftsleiter; Sorgfaltspflicht; Compliance; Compliance-Organisation; Risikomanagementsystem; Ö-Normen.

I. Einleitung

Die österreichische Rechtsordnung sieht keine generelle Verpflichtung zur Installierung einer Compliance-Organisation vor. Wenige ausdrückliche Anordnungen bestehen im Finanzdienstleistungssektor: So verpflichten § 15 InvFG¹ und § 18 WAG² Finanzdienstleistungsunternehmen zur Einrichtung einer wirksamen und unabhängigen Compliance-Organisation, die der Art, dem Umfang und der Komplexität der Geschäfte entsprechen muss. Auch börsennotierte Unternehmen haben gem § 82 Abs 5 BörseG organisatorische Vorkehrungen zur Unterbindung von Insiderhandel zu treffen und nach dem Österreichischen Corporate Governance Kodex (ÖCGK) ein internes Risikomanagementsystem zu installieren.³ Die Notwendigkeit zur Errichtung einer Compliance-Organisation ergibt sich schließlich für Unternehmen, die an einer öffentlichen Auftragsvergabe teilnehmen: Geeignete Maßnahmen zum Beleg der „beruflichen Zuverlässigkeit“, die zur Teilnahme am Vergabeverfahren berechtigt, sind gem § 73 Abs 2 BVerG⁴ ein qualitativ hochwertiges Berichts- und Kontrollwesen, die Einschaltung eines internen Organs zur regelmäßigen Überprüfung der Einhaltung der maßgeblichen Vorschriften und interne Haftungs- und Schadenersatzre-

* Postdoc-Ass. Dr. Mona Philomena Ladler, Bakk. lehrt am Institut für Rechtswissenschaften an der Universität Klagenfurt. Der Beitrag basiert auf dem am 11. 12. 2015 in Graz im Rahmen der Tagung „Recht und IT: Compliance-Management. Standards – Tools – Haftung“ gehaltenen Vortrag der Verfasserin. Für hilfreiche Anmerkungen gebührt Univ.-Prof. Dr. Christoph Kietabl aufrichtiger Dank.

1 Investmentfondsgesetz (InvFG) 2011 BGBl I 2011/77.

2 Wertpapieraufsichtsgesetz (WAG) 2007 BGBl I 2007/60.

3 Vgl Regeln 9, 15, 40, 70 ÖCGK idF Jänner 2015.

4 Bundesvergabegesetz (BVerG) 2006) BGBl I 2006/17.

gelungen.⁵ Im allgemeinen Gesellschafts- und Unternehmensrecht finden sich hingegen keine Bestimmungen zur Einrichtung einer Compliance-Organisation. Deshalb fehlt es auch an allgemeinen gesetzlichen Anhaltspunkten, wie ein Compliance Management System (CMS) zu organisieren ist. Entsprechende Hilfestellungen zur Organisation eines CMS bieten von nationalen und internationalen Normungsinstitutionen veröffentlichte Standards, wie die ONR 192050 bzw die ISO 19600.⁶ Bei Erfüllung der nach ONR 192050 bzw ISO 19600 vorgegebenen Kriterien⁷ kann einem Unternehmen ein zeitlich befristetes Zertifikat durch eine Zertifizierungsstelle zuerkannt werden, welches die Qualität und Funktionstüchtigkeit seines CMS belegt.⁸

Die zivil- und gesellschaftsrechtlichen Folgen einer solchen Zertifizierung sind bislang ungeklärt. In diesem Beitrag werden die Rechtsqualität der CMS-Standards und die Haftungsfolgen einer Zertifizierung untersucht. Darüber hinaus wird analysiert, ob auch ohne Zertifizierung eine Pflicht zur Orientierung an CMS-Standards bestehen kann.

II. Ausgangslage

A. Compliance als Leitungsverantwortung

Ungeachtet der rudimentären gesetzlichen Ausgestaltung von Compliance-Organisationen wird eine generelle Verpflichtung zu Compliance einhellig bejaht.⁹ Es entspricht einer ordnungsgemäßen Unternehmensführung iSd § 25 GmbHG bzw §§ 70 iVm 84 AktG, die Einhaltung gesetzlicher und vertraglicher Verpflichtungen der Gesellschaft sicherzustellen.¹⁰ Der Geschäftsführer unterliegt nicht bloß in Ausübung seiner eigenen Tätigkeit einer Legalitätspflicht, vielmehr trifft ihn auch eine horizontale und vertikale Überwachungspflicht. Die horizontale Überwachung ist Ausfluss der Gesamtverantwortung des einzelnen Organmitgliedes für die Geschäftsführung und verpflichtet zur gegenseitigen Kontrolle bei Ressortverteilung.¹¹ Die vertikale Überwachung erstreckt

5 Weiterführend *Gölles/Makarius*, Prüfpflicht öffentlicher Auftraggeber bei Unzuverlässigkeit und Chance auf „Selbstreinigung“ für Unternehmer, RPA 2014, 185.

6 *Dürager*, Die rechtlichen Fallstricke bei der Überwachung und Durchsetzung einer Compliance-Organisation, ZIR 2013, 339 (341); *Hussian*, Compliance-Management-System nach der ONR 192050, bau aktuell 2014, 163.

7 ZB Identifikation und Neubewertung konkreter Compliance-Risiken; Einrichtung einer Compliance-Funktion; Definition von Compliance-Zielen; interne Bewusstseinsbildung und Schulungsmaßnahmen etc: Compliance management systems – Guidelines, ISO 19600:2014(E); verfügbar unter Austrian Standards, Compliance Management Systeme: Zertifizierungsschema https://www.austrian-standards.at/fileadmin/user/bilder/downloads-produkte-und-leistungen/Zertifizierungsschema_Compliance.pdf (abgefragt am 25. 1. 2016; in der Folge kurz: CMS-Zertifizierungsschema).

8 Details dazu erläutert der Beitrag von *Jonas*, Die Internationale Norm ISO 19600 Compliance Management Systems – Inhalte und Zertifizierung, ALJ 2016, 37.

9 *Kalss* in *Kalss/Nowotny/Schauer* (Hrsg), Österreichisches Gesellschaftsrecht (2008) Rz 3/334. *Knafl*, Einführung von Compliance-Systemen (2014) 41 f; *Dürager*, ZIR 2013, 340.

10 § 22 Abs 1 GmbHG verpflichtet den Geschäftsführer einer GmbH, ein Rechnungswesen und internes Kontrollsystem einzurichten. Eine inhaltsgleiche Anordnung besteht gem § 82 AktG für den Vorstand einer AG. Das interne Kontrollsystem umfasst nach dem Willen des Gesetzgebers „sämtliche aufeinander abgestimmte Methoden und Maßnahmen in einem Unternehmen [...], die dazu dienen, das Vermögen zu sichern, die Genauigkeit und Zuverlässigkeit der Abrechnungsdaten zu gewährleisten und die Einhaltung der vorgeschriebenen Geschäftspolitik zu unterstützen.“ Dementsprechend ist die Etablierung von Kontrollmechanismen, die die Liquidität der Gesellschaft sicherstellen und überwachen, verpflichtend. § 22 GmbHG bzw § 82 AktG beziehen sich lediglich auf die Einrichtung eines Rechnungswesens; eine weitreichende Anordnung zur Installierung einer Compliance-Organisation ist nach hA daraus nicht ableitbar. *Strasser* in *Jaborlegg/Strasser* (Hrsg), Kommentar zum Aktiengesetz⁵ (2011) §§ 77–84 Rz 15; *Reich-Rohrwig* in *Straube/Ratka/Rauter* (Hrsg), GmbHG (2015) § 25 Rz 16; *Feltl/Pucher*, Corporate Compliance im österreichischen Recht – Ein Überblick, wbl 2010, 269; vlg auch *Koppensteiner/Rüffler* in *Koppensteiner/Rüffler* (Hrsg), GmbH-Gesetz Kommentar³ (2007) § 22 Rz 2.

11 *Kalss* in *Kalss/Nowotny/Schauer* Rz 3/347; *Strasser* in *Jaborlegg/Strasser*, AktG⁵ § 70 Rz 41.

sich auf die Überwachung, Anleitung und Kontrolle nachgeordneter Mitarbeiter.¹² Um dieser Überwachungspflicht gerecht zu werden, ist eine entsprechende Organisation des Unternehmens erforderlich.¹³ So setzt die Gewährleistung der Einhaltung verwaltungsrechtlicher Vorschriften gem § 9 Abs 1 VStG nach stRsp die Etablierung eines wirksamen Kontrollsystems voraus. Interne Schulungen oder Weisungen an untergeordnete Mitarbeiter sind nicht ausreichend; auch eine nachträgliche Überprüfung bereits gesetzten Verhaltens wird den Anforderungen an die (verwaltungsrechtliche) Legalitätspflicht nicht gerecht. Geschäftsleiter treffen vielmehr präventive Überwachungspflichten, deren wirksame Wahrnehmung die Installierung eines entsprechenden Risikomanagementsystems erfordert.¹⁴

In der Wahl der zu setzenden Maßnahmen haben Geschäftsleiter allerdings einen Ermessensspielraum.¹⁵ Die interne Organisation hat den Anforderungen des Unternehmens zu entsprechen; sie ist branchen- und unternehmensspezifisch. Maßgebliche Kriterien sind insb die Größe des Unternehmens, die Branche, das Geschäftsmodell sowie die konkrete Risikosituation im Unternehmen unter Berücksichtigung vergangener Missstände.¹⁶ Anhaltspunkte für die Ausübung dieses Organisationsermessens finden sich nur in Sondergesetzen; und selbst diese erlauben es aufgrund ihrer Divergenz nicht, allgemeingültige Anforderungen an die interne Überwachungsarchitektur abzuleiten.¹⁷ Abhängig von der Art des Unternehmens (Börsennotierung) bzw Geschäftsfeld (Finanzdienstleistungssektor) und Kontrahierungspartner (Vergaberecht) ist zwar eine Verpflichtung zur Installierung eines CMS zu bejahen. Die Ausgestaltung des CMS ist aber auch in diesen Fällen an das konkrete Unternehmen anzupassen.¹⁸ Auch sind diese Vorgaben nicht uneingeschränkt auf alle Unternehmen zu übertragen: Insb in kleinen Einheiten kann die Einrichtung einer gesonderten Compliance-Funktion unterbleiben, sofern die Legalitätskontrolle auch durch die Geschäftsführung selbst wahrgenommen werden kann.

12 Reich-Rohrwig in Straube/Ratka/Rauter, GmbHG § 25 Rz 48; Nowotny in Doralt/Nowotny/Kalss (Hrsg), Kommentar zum Aktiengesetz² (2012) § 70 Rz 17.

13 Feltl/Pucher, wbl 2010, 270; Strauss/Hermann, Die Pflicht zur Einführung von Compliance-Management-Systemen und der Aufsichtsrat, Aufsichtsrat aktuell 2014/6, 8; deutlich zum dt Recht LG München 10. 12. 2013, 5 HK O 1387/10.

14 VwGH 24. 3. 2015 2013/0054; VwGH 30. 6. 2011 2011/03/0078; zum Arbeitgeber VwGH 18. 8. 2015 Ro 2015/11/0003. Reich-Rohrwig in Straube/Ratka/Rauter, GmbHG § 25 Rz 490.

15 Feltl/Pucher, wbl 2010, 270 f; Knafl, Compliance-Systeme 48; Schirmer/Uitz, Compliance-Maßnahmen zur Reduktion der Haftungsrisiken von Vorstandsmitgliedern, RdW 2010, 200 (201); zum dt Recht Sünner, Von der Sorge für gesetzeskonformes Verhalten – Zugleich eine Besprechung des ISO-Entwurfs 19600, CCZ 2015, 2.

16 Dürager, ZIR 2013, 341; Strauss/Hermann, Aufsichtsrat aktuell 2014/6, 10.

17 So ordnen § 15 InvFG bzw § 18 WAG die Einrichtung einer dauerhaften und unabhängigen Compliance-Funktion an. Diese besteht aus einem Compliance-Beauftragten und allenfalls weiteren betrauten Personen, die über die notwendige Sachkenntnis verfügen. Der Compliance-Beauftragte trägt die Verantwortung für die Compliance-Funktion und unterliegt Berichtspflichten gegenüber der Geschäftsleitung. Um die Funktionsstüchtigkeit der Compliance-Funktion sicherzustellen, sind den mit der Funktion betrauten Personen die notwendigen Befugnisse, Ressourcen und Informationszugänge einzuräumen. § 73 Abs 2 BVergG setzt gar nur ein „qualitatives“ Kontrollwesen voraus; die Anforderungen an die interne Compliance-Funktion oder die Funktionsweise des internen Haftungs- und Entschädigungsregimes werden nicht weiter konkretisiert. Nach dem ÖCGK hat der Vorstand die „geeigneten Vorkehrungen“ zur Sicherstellung der Einhaltung der Gesetze zu treffen (Regel 15 ÖCGK). Zudem sind „die wesentlichen eingesetzten Risikomanagement-Instrumente in Bezug auf nicht-finanzielle Risiken“ in den Konzernlagebericht aufzunehmen (Regel 70 ÖCGK. Diesbezüglich genügt eine allgemeine Beschreibung der eingesetzten Risikomanagementsysteme; eine Darstellung der Funktionsfähigkeit ist nicht erforderlich: Interpretation zum ÖCGK, zu Regel 70) und ist der AR über alle relevanten Fragen der Geschäftsentwicklung, einschließlich des Risikomanagements, zu informieren (Regel 9, 40 ÖCGK).

18 Siehe § 18 Abs 4 UAbs 2 WAG bzw § 15 Abs 4 InvFG.

Eine Compliance-Organisationspflicht steht daher immer unter dem Vorbehalt einer Einzelfallbetrachtung.¹⁹

Eine ungenügende Compliance-Organisation stellt einen Sorgfaltswiderruß iSd § 25 GmbHG bzw § 70 iVm § 84 AktG dar. So kann eine Verletzung der Überwachungspflicht eine Zurechnung des Verhaltens der Mitarbeiter zum Geschäftsführer bzw Vorstand bewirken.²⁰ Geschäftsleiter haben ihre Aufgaben gem § 25 GmbHG bzw § 84 AktG mit der Sorgfalt eines ordentlichen Geschäftsmannes wahrzunehmen. Der Sorgfaltswiderruß ist objektiv,²¹ die Anforderungen, die an einen ordentlichen Geschäftsmann gestellt werden, sind stets im Anlassfall unter Berücksichtigung der Art des Unternehmens, der Größe oder der wirtschaftlichen Lage zu ermitteln.²² Eine Haftung des Geschäftsleiters tritt – bei Vorliegen der sonstigen zivilrechtlichen Voraussetzungen – bei eklatantem Überschreiten des objektiven Sorgfaltswiderrusses ein.²³ Anspruchsberechtigt ist grundsätzlich die Gesellschaft,²⁴ in Einzelfällen kann auch eine Haftung gegenüber Gesellschaftsgläubigern (§ 25 Abs 5 GmbHG bzw § 84 Abs 5 AktG) oder Aktionären (deliktisch) bestehen.²⁵ Den Freibeweis für sorgfältiges Handeln haben die Geschäftsleiter zu erbringen.²⁶

B. Rechtliche Einordnung und Funktion der ISO 19600

CMS-Standards, wie ISO 19600 und ONR 192050, können eine Hilfestellung in Ausübung des Organisationsermessens bieten und damit das Haftungsrisiko des Geschäftsleiters reduzieren. Die ISO 19600 und ONR 192050 wurden von privaten Normungsinstitutionen, der International Standardization Organization (ISO) bzw dem Austrian Standards Institute (ASI), veröffentlicht. Diese Standards sind kein Gesetzesrecht. Ihrer Rechtqualität nach sind sie mit Ö-Normen vergleichbar,²⁷ die den aktuellen Stand der Technik repräsentieren und eine Zusammenfassung der üblichen Sorgfaltsanforderungen aus dem Wirtschaftsleben darstellen.²⁸ Ö-Normen sind rechtlich unverbindlich und haben nur dann allgemeine Geltung, wenn sie durch Gesetz oder Verordnung für verbindlich erklärt wurden.²⁹ Darüber hinaus können Ö-Normen durch Parteienvereinbarung (auch konkudent) zum Vertragsbestandteil werden und auf diese Weise Bindungswirkung entfalten.³⁰ Doch auch ohne eine entsprechende gesetzliche oder vertragliche Verbindlicherklärung können Ö-Normen *de facto* Geltung erlangen: Werden Ö-Normen durch Übung der beteiligten Verkehrskreise zum Handelsbrauch oder zur Verkehrssitte, sodass in künftigen Fällen mit einer Anwendung zu rechnen ist, sind sie nach StRp als Auslegungsmaxime heranzuziehen.³¹

19 Feltl/Pucher, wbl 2010, 270 f; Knafl, Compliance-Systeme 48, aA Strauss/Hermann, Aufsichtsrat aktuell, 10.

20 Koppensteiner/Rüffler in Koppensteiner/Rüffler, GmbHG³ § 25 Rz 10 mwN.

21 Koppensteiner/Rüffler in Koppensteiner/Rüffler, GmbHG³ § 25 Rz 14.

22 Völk, Der österreichische Corporate-Governance-Kodex im Licht der §§ 70 und 84 AktG, GesRZ 2003, 73.

23 Reich-Rohrwig in Straube/Ratka/Rauter, GmbHG § 25 Rz 36.

24 § 25 Abs 2 GmbHG; § 84 Abs 2 AktG.

25 Jabornegg in Jabornegg/Strasser (Hrsg), Kommentar zum Aktiengesetz⁵ (2011) § 84 Rz 101.

26 § 84 Abs 2 Satz 2 AktG.

27 ONR sind als bloße technische Regeln eine Vorstufe zu Ö-Normen: Hauer, Rechtliche Grenzen der Normung, ZTR 2014, 102.

28 StRp OGH 15. 4. 1998, 3 Ob 70/98k; OGH 22. 10. 1999, 1 Ob 278/98h; OGH 27. 3. 2001, 1 Ob 262/00m; OGH 8. 7. 2015, 1 Ob 79/15x.

29 § 9 Normengesetz 2016 BGBl I 2015/153; Hauer, ZTR 2014, 102.

30 Graf in Kletečka/Schauer (Hrsg), ABGB-ON^{1,02} § 864a Rz 11 mwN (Stand 19. 5. 2015, rdb.at); Rummel in Rummel (Hrsg), Kommentar zum Allgemeinen Bürgerlichen Gesetzbuch³ (2002) § 861 Rz 12.

31 StRp, zuletzt OGH 6. 8. 2015, 2 Ob 223/14d; RIS-Justiz RS0038622; zu verfassungsrechtlichen Bedenken bspw Hauer, ZTR 2014, 102.

Auch der ISO-Standard 19600 entfaltet keine rechtliche Bindungswirkung, sondern dient primär als „Anhaltspunkt“³² oder „Orientierungsstandard“³³. Er erfordert zu seiner Geltung mangels einer gesetzlichen oder behördlichen Verbindlicherklärung eine vertragliche Vereinbarung. Bei entsprechender Verbreitung könnte darüber hinaus eine den Ö-Normen vergleichbare faktische Bindungswirkung eintreten.

Es liegt daher grundsätzlich im Ermessen der Geschäftsleitung, die interne Überwachungsarchitektur in Einklang mit ISO 19600 zu gestalten. Dies ergibt sich sowohl aus dem Organisationsermessen der Geschäftsleitung, als auch aus der mangelnden Bindungswirkung des Standards. Anderes gilt bei Erwerb einer Zertifizierung (dazu gleich im Folgenden unter Punkt 3.) bzw bei Bejahung einer faktischen Geltung (dazu im Folgenden unter Punkt 4.): Entschließt sich die Geschäftsleitung zum Aufbau eines CMS auf der Grundlage von ISO 19600 und zu einer Zertifizierung desselben, entfaltet der Standard Bindungswirkung. Darüber hinaus könnte bei Vorliegen eines Handelsbrauches auch eine faktische Geltung des ISO-Standards 19600 eintreten. Dies würde das Organisationsermessen der Geschäftsleitung in weiterer Folge reduzieren, weil ein dem Standard entsprechendes CMS erforderlich würde.

III. Rechtslage bei einer CMS-Zertifizierung

A. Rechtliche Einordnung einer CMS-Zertifizierung

Die Geltung der ONR 192050 bzw ISO 19600 wird bei einer Zertifizierung vertraglich von den Parteien vereinbart. Eine Zertifizierung durch die Zertifizierungsstelle von Austrian Standards (AS + C) ist zivilrechtlich als Vertrag zwischen der Gesellschaft und AS + C einzuordnen,³⁴ dem die ISO 19600 bzw ONR 192050 zugrunde gelegt werden.³⁵ Sie entfalten demnach Bindungswirkung zwischen den Parteien, sodass Handlungen der Gesellschaft entgegen der Zertifizierung eine Verletzung der vertraglichen Verpflichtungen darstellen. Dies kann in weiterer Folge zu einer Zurückziehung des Zertifikats durch AS + C führen.³⁶ Aus dem Zertifizierungsverfahren entstandene Kosten sind von der Gesellschaft zu tragen.³⁷

Doch auch außerhalb des Vertragsverhältnisses sind mit einer CMS-Zertifizierung besondere Verpflichtungen verbunden. Zu denken ist insb an § 2 Abs 3 Z 2 UWG, welcher der Nichteinhaltung von Verpflichtungen aus einem Verhaltenskodex, dem sich der Unternehmer freiwillig unterworfen hat, Irreführungseignung zuerkennt. Irreführung ist gegeben, wenn ein Unternehmer auf die Geltung eines Verhaltenskodizes verweist (lit a) und ein Marktteilnehmer aufgrund dieser Annahme zu einer geschäftlichen Entscheidung veranlasst wurde. Dies setzt voraus, dass der Verhaltenskodex eindeutige Verpflichtungen enthält, deren Einhaltung nachprüfbar ist (lit b).³⁸ Unzulässig ist nicht bloß die Nichteinhaltung von freiwillig auferlegten Verpflichtungen, sondern auch die unrichtige Behauptung eines Unternehmers, einen Verhaltenskodex unterzeichnet zu

32 Zur ONR 192050 *Dürager*, ZIR 2013, 341.

33 Zur ONR 192050 *Busch/Hjertonsson*, Sieben Elemente eines effizienten und wirksamen Compliance-Management-Systems, CFO aktuell 2013, 96 (96).

34 Punkt 11 CMS-Zertifizierungsschema.

35 Punkt 3.1 CMS-Zertifizierungsschema iVm Anhang A, B.

36 Punkt 3.10 CMS-Zertifizierungsschema.

37 Anhang C, Punkt 2 und 11 CMS-Zertifizierungsschema.

38 Siehe *Anderl/Appel* in *Wiebe/Kodek* (Hrsg), UWG² (2012) § 2 UWG Rz 472 ff.

haben.³⁹ Jedenfalls irreführend ist zudem die Verwendung eines Gütesiegels oder Qualitätskennzeichens ohne erforderliche Genehmigung⁴⁰ und die unrichtige Behauptung, dass ein Unternehmen von einer öffentlichen oder privaten Stelle bestätigt, gebilligt oder genehmigt worden sei.⁴¹

Wird den Verpflichtungen aus der CMS-Zertifizierung nicht nachgekommen, bei Handlungen im geschäftlichen Verkehr aber auf das Zertifikat verwiesen, ist eine Irreführung gem § 2 UWG gegeben. Eine CMS-Zertifizierung setzt die Erfüllung eindeutiger Verpflichtungen voraus, deren Einhaltung auch nachprüfbar ist. Wird das CMS-Zertifikat im geschäftlichen Verkehr verwendet, obwohl keine Zertifizierung erlangt wurde oder ist die Zertifizierung abgelaufen, liegt eine irreführende Geschäftspraktik gem Z 2 bzw Z 4 des Anhanges zum UWG vor. Dies kann in weiterer Folge zu Unterlassungs- und Schadenersatzpflichten der Gesellschaft führen.⁴²

B. Haftung bei CMS-Zertifizierung

Die Zertifizierung bewirkt im Außenverhältnis eine vertragliche Verpflichtung der Gesellschaft. Im Innenverhältnis obliegt es der Geschäftsleitung, die Umsetzung der gesetzlichen und vertraglichen Verpflichtungen der Gesellschaft sicherzustellen. Eine Zertifizierung ist daher untrennbar mit der Frage nach den Pflichten und der Haftung der Geschäftsführung verknüpft.

1. Haftungserhöhung

Eine Zertifizierung bewirkt zunächst eine Haftungserhöhung der Geschäftsleitung, weil der Umfang der einzuhaltenden Verpflichtungen umfassender wird. Wurde ein CMS-Zertifikat erworben, ist die Geschäftsleitung im Rahmen ihrer Legalitätspflicht verpflichtet, sich vertragsgemäß zu verhalten; maW sind die Umstände, die zu einer Zertifizierung geführt haben, aufrechtzuerhalten. Handlungen entgegen des Vertrages können eine Pflichtverletzung durch die Geschäftsleitung begründen und in weiterer Folge zu einer Haftung führen.

Eine Haftung des Geschäftsleiters kann zudem aus sondergesetzlichen Verpflichtungen resultieren: Wird ein Zertifikat irreführend genutzt, ist die Gesellschaft nach dem UWG zu sanktionieren. Da jedoch der Geschäftsleiter im Innenverhältnis für die Durchsetzung der gesetzlichen Verpflichtungen verantwortlich ist, ist der Geschäftsleiter gegenüber der Gesellschaft zur Haftung heranzuziehen. Schadenersatzpflichten der Gesellschaft können daher beim Geschäftsleiter regressiert werden.⁴³

2. Haftungsminderung

Zugleich kann eine CMS-Zertifizierung eine erhebliche Reduktion des Haftungsrisikos der Geschäftsleitung bewirken. Einer Zertifizierung liegt der Aufbau eines CMS anhand von Leitlinien zugrunde, welche die Geschäftsleitung in Wahrnehmung ihrer Legalitäts- und Organisationsverantwortung unterstützen. Die ISO 19600 bzw das CMS-Zertifizierungsschema enthalten konkrete Handlungsanweisungen, wodurch Risiken in der Gesellschaft leichter erkannt und unterbunden werden

39 Z 1 Anhang UWG.

40 Z 2 Anhang UWG.

41 Z 4 Anhang UWG.

42 § 1 Abs 5 UWG.

43 Siehe *Jabornegg in Jabornegg/Strasser, AktG*⁵ § 84 Rz 103 mwN.

können.⁴⁴ Darüber hinaus werden potenzielle Mängel im CMS durch externe Auditors aufgezeigt. Im Zuge des Zertifizierungsverfahrens sind zwei Überprüfungen des CMS durchzuführen⁴⁵ und während aufrechter Zertifizierung jährlich zu kontrollieren.⁴⁶ Hierdurch können Risiken identifiziert werden, die „betriebsblinde“ Leitungsorgane uU übersehen.

Zudem kann eine CMS-Zertifizierung eine Vermutungswirkung für sorgfältiges Handeln begründen. Der Geschäftsleiter ist seinem Organisationsermessen ordnungsgemäß nachgekommen, weil er ein CMS aufgebaut hat, das international erarbeiteten Standards entspricht. Darüber hinaus wurde dieses zertifiziert, sodass der Beweis, dass in Einklang mit der branchenüblichen Sorgfalt gehandelt wurde, leichter gelingen wird.⁴⁷

3. Sorgfaltsminderung?

a. Normgerecht, aber nicht fehlerfrei

Eine Zertifizierung darf aber nicht dahingehend verstanden werden, dass die Sorgfaltspflicht damit begrenzt ist. Zwar indiziert eine normgerechte Herstellungsart nach stRsp die Fehlerfreiheit eines Produkts,⁴⁸ doch ist diese rechtliche Vermutung in Bezug auf zertifizierte CMS zu relativieren. Zunächst wird eine Zertifizierung nur für einen von der Gesellschaft definierten Geltungsbereich ausgestellt.⁴⁹ Ein CMS-Zertifikat kann sich daher durchaus auch nur auf einen Teilbereich der Compliance-Organisation beziehen und nicht sämtliche zu überwachenden Bereiche und Materien umfassen. Das CMS-Zertifikat belegt dann bloß, dass dieser Teilbereich in Einklang mit der ISO 19600 gestaltet wurde.

Zudem ist bei einem mangelhaften Produkt oder Werk problemlos feststellbar, ob der zugrundeliegenden Ö-Norm/ISO entsprochen wurde. Wird etwa ein Fenster in Einklang mit der entsprechenden Ö-Norm hergestellt, verfügt es über gewisse technische Eigenschaften, wie eine Dichtung. Ist die Dichtung wasserundurchlässig, wurde nicht dem aktuellen Stand der Technik entsprechend gehandelt und ist das Produkt fehlerhaft. Alle Fenster-Hersteller haben dieselben technischen Eigenschaften zu erfüllen, ungeachtet der Größe oder technischen Ausstattung des Unternehmens. Unternehmen als Organisationen sind hingegen nicht mit Produkten vergleichbar. Leitungsorgane unterliegen einem Ermessensspielraum, wie das Unternehmen zu organisieren ist; die konkrete Ausgestaltung eines CMS ist stets an das Unternehmen anzupassen. Es ist daher immer eine Einzelfallbetrachtung vorzunehmen, ob das CMS den Anforderungen eines Unternehmens genügt. Mechanismen, die sich in einem Unternehmen bewährt haben, sind kein Garant für die Unterbindung von Gesetzesverstößen in anderen Unternehmen. Compliance ist von der Unternehmenskultur abhängig: So können sich etwa Whistleblowing-Systeme in manchen Unternehmen als wichtiger Teil der Aufdeckung und Ahndung unternehmensinterner Verstöße erweisen, in anderen Unternehmen aber kaum genutzt werden.

44 Vgl Dürager, ZIR 2013, 341.

45 Punkt 3.3 CMS-Zertifizierungsschema.

46 Punkt 3.6 CMS-Zertifizierungsschema.

47 Vgl Ebmer, Haftungsbefreiende Wirkung von Compliance-Management-Systemen für Verbände und Leitungsorgane, bau aktuell 2014, 205.

48 OGH 28. 6. 1995, 3 Ob 547/95; 16. 7. 1998, 6 Ob 157/98a; 23. 9. 2004, 6 Ob 73/04k.

49 Punkt 3.1.3 CMS-Zertifizierungsschema; Die Rosenbauer International AG hat etwa die Risikofelder „Korruption“ und „Wettbewerbsrecht“ zertifiziert: <https://certificates.austrian-standards.at/certificate?1> (abgefragt am 25. 1. 2016).

Vor diesem Hintergrund erscheint es auch problematisch, den Sorgfaltsmäßigstab anhand allgemeiner Compliance-Standards zu konkretisieren. Aufgrund der Verschiedenartigkeit und Vielfältigkeit unternehmerischer Tätigkeit kann keine allgemeingültige Lösung für die Organisation von Compliance gefunden werden. Dies zeigt auch der Aufbau und Umfang der ISO 19600 selbst: So haben Unternehmen etwa eine von den individuellen Bedürfnissen abhängige unternehmensspezifische Analyse der eigenen Risikosituation vorzunehmen.⁵⁰ Welche möglichen Risiken erfasst sein könnten, wird hingegen nicht vorgegeben. Selbst in Unternehmen, für die ein CMS gesetzlich vorgeschrieben ist, sind kaum pauschale Vorgaben möglich. So werden auch die dem WAG oder InvFG unterliegenden Rechtsträger von einzelnen Compliance-Organisationsanforderungen ausgenommen, sofern ein Nachweis der Unverhältnismäßigkeit erbracht wird.⁵¹ Die ON 192050 und ISO 19600 sind in diesem Sinne nicht mit anderen technischen Standards, wie etwa zur Produktsicherheit und technischer Eigenschaften, vergleichbar.

Ein Geschäftsleiter kann sich demnach nicht unter Berufung auf eine ISO-Zertifizierung von der Haftung freizeichnen. Selbst bei Handeln in Einklang mit der Norm und einer Zertifizierung ist eine Haftung der Geschäftsleiter nicht ausgeschlossen.⁵²

b. Kollision mit Vorstandspflichten?

Eine Zertifizierung kann zudem in einem Spannungsverhältnis zu kardinalen Vorstandspflichten stehen. Insb kann eine *Moral-hazard-Problematik* auftreten: Indem Geschäftsleiter ihre Legalitätsverantwortung auf eine Compliance-Funktion übertragen, wird die eigenverantwortliche Überwachung durch die Geschäftsleiter vermeintlich reduziert. Sie wiegen sich in falscher Sicherheit, dass eine Legalitätskontrolle ohnehin vorgenommen würde. Geschäftsleiter trifft aber immer die Gesamtverantwortung für die Legalitätskontrolle, einschließlich Compliance.⁵³ Auch im Falle einer Ressortverteilung erfordert die horizontale Überwachungspflicht eine gegenseitige Kontrolle anderer Vorstandsmitglieder, die durch Informations- und Auskunftsrechte ausgeübt wird.⁵⁴ Die Compliance-Funktion muss folglich in ihrer Tätigkeit überwacht werden, andernfalls eine Solidarhaftung der Geschäftsleitung eintreten könnte.

Eine umfassende Überwachung durch den Vorstand könnte aber daran scheitern, dass Compliance-Funktionen unabhängig sind.⁵⁵ Dies schließt Weisungen seitens der Geschäftsleitung an Compliance-Beauftragte aus. Compliance-Funktionen sind zudem mit den für die Wahrnehmung ihrer Tätigkeit notwendigen Informationen auszustatten bzw sind die notwendigen Informationsrechte einzuräumen.⁵⁶ Der Vorstand unterliegt aber gem § 84 Abs 1 Satz 2 AktG einer Geheimhaltungspflicht. Eine Weitergabe von Informationen ist nur im Interesse der Gesellschaft zulässig.⁵⁷ Die Errichtung eines CMS kann daher mit wesentlichen Vorstandspflichten kollidieren. Eine „Übererfüllung“ der Legalitätspflicht, im Sinne einer Ausstattung der Compliance-Funktion mit zu weitreichenden Befugnissen, könnte letztlich sogar eine Sorgfaltspflichtverletzung des Vorstandes begründen.

50 Punkt A.4.10 CMS-Zertifizierungsschema.

51 § 18 Abs 4 UAbs 2 InvFG; § 15 Abs 4 WAG.

52 So auch *Hussian*, bau aktuell 2014, 163.

53 So zuletzt VwGH 11. 9. 2015, 2013/17/0485; 4. 7. 2008, 2008/17/0072.

54 *Jabornegg in Jabornegg/Strasser*, AktG⁵ § 70 Rz 41.

55 § 18 InvFG; § 15 WAG; Punkt A.5.12. CMS-Zertifizierungsschema.

56 Punkt A.5.15. Z 3 CMS-Zertifizierungsschema.

57 Eine Grenze bildet nach hL die Weitergabe von Aufsichtsratsprotokollen oder Protokollen von Vorstandssitzungen.

Kalss/Schörghofer, Corporate Compliance und Gesellschaftsrecht, in *Lucius/Oppitz/Pachinger*, Compliance im Finanzdienstleistungsbereich (2010) Kapitel 1.

IV. Rechtslage ohne CMS-Zertifizierung

A. ISO 19600 als Handelsbrauch?

Wie dargelegt, besteht im Allgemeinen⁵⁸ keine generelle gesetzliche Verpflichtung zum Aufbau einer CMS-Organisation. Vielmehr verfügen Geschäftsleiter über ein Organisationsermessen, das eine andere, als nach ISO 19600 vorgegebene Überwachungsarchitektur erlaubt. Fraglich ist, ob dennoch ein Druck zur Befolgung der ISO 19600 bestehen könnte, zumal Ö-Normen nach stRsp auch ohne entsprechende gesetzliche oder vertragliche Verbindlicherklärung als Handelsbrauch *de facto* Geltung erlangen können.⁵⁹

Ein Handelsbrauch (bzw Unternehmensbrauch) ist eine unternehmerische Verkehrssitte. Er dient gem § 346 UGB als Interpretationsmaxime, wonach Handlungen und Unterlassungen von Unternehmern, im Hinblick auf die im Geschäftsverkehr geltenden Gewohnheiten und Gebräuche, auszulegen sind. Zudem wird ein Handelsbrauch als Vertragsergänzung bei mangelnder Regelung herangezogen.⁶⁰ Damit ein Handelsbrauch vorliegt, muss eine Verhaltensweise innerhalb eines bestimmten Geschäftskreises für eine gewisse Zeit freiwillig geübt werden. Das Tatbestandsmerkmal der Übung erfordert eine entsprechende Verbreitung einer Verhaltensweise. Hiervon ist auszugehen, wenn „ein ganz überwiegender Teil“ der Verkehrskreise die Verhaltensweise befolgt.⁶¹ Wird etwa in einem Werkvertrag nichts bezüglich der technischen Eigenschaften eines Werks vereinbart, so ist das Werk so zu erstellen, wie es üblich und angemessen ist; dabei sind die anerkannten Regeln des Fachs, einschließlich Ö-Normen, anzuwenden. Der Werkunternehmer ist seinem Vertragspartner gegenüber verpflichtet, ein Werk zu liefern, das der relevanten Ö-Norm entspricht.⁶²

Auch einer ISO 19600-Zertifizierung liegt ein Vertrag mit der Zertifizierungsstelle zu Grunde. Bei fehlender Vereinbarung könnte der ISO-Standard als Handelsbrauch der Auslegung des Zertifizierungsvertrages dienen bzw vertragsergänzend wirken. Eine solche Entwicklung ist derzeit aber nur wenig wahrscheinlich. Aktuell haben erst drei Unternehmen ein CMS-Zertifikat beantragt und erlangt.⁶³ Es ist daher von keiner Verhaltensweise auszugehen, die von einem überwiegenden Teil der Verkehrskreise befolgt wird. Selbst bei Berücksichtigung des Umstandes, dass es sich bei CMS-Standards um ein relativ junges Konzept handelt, ist nicht von einer künftigen Herausbildung eines Handelsbrauches auszugehen. Zwar würde es genügen, dass nur Unternehmen einer Branche oder eines Geschäftszweiges eine Verhaltensweise üben. So wäre es etwa denkbar, dass andere Energiedienstleister dem Beispiel der KELAG folgen und sich ein (auch regionaler) Handelsbrauch für Energieunternehmen entwickelt. Dem stehen aber inhomogene Organisationsstrukturen von Unternehmen entgegen, zumal insb kleine Unternehmen uU gar kein derart umfassendes CMS, wie es von ISO 19600 vorgegeben wird, benötigen.⁶⁴

58 Zu den Ausnahmen vgl oben unter Punkt 1.

59 RIS-Justiz RS0038622; RS0038609.

60 RIS-Justiz RS0102364; RS0062008.

61 Kramer/Rauter in Straube (Hrsg), Wiener Kommentar zum UGB, 31. Lfg (2011) § 346 Rz 10 mwN. Die WKÖ geht bei Erhebungen von einem Handelsbrauch aus, wenn Drei Viertel der befragten Verkehrsteilnehmer die Verhaltensweise üben. Übersicht über Handelsbräuche <https://www.wko.at/Content.Node/Interessenvertretung/Wirtschaftsrecht/Handelsbrauch-Liste.html> (abgefragt am 25. 1. 2016).

62 OGH 22. 6. 2010, 10 Ob 24/09s; 17. 6. 1986, 4 Ob 356/86; Krejci, Unternehmensrecht⁴ (2008) 27.

63 KELAG-Kärntner Elektrizitäts-Aktiengesellschaft, Rosenbauer International AG, Magistrat der Stadt Wien, Magistratsabteilung 48, https://certificates.austrian-standards.at/FBCC_Faibusiness_Certification (abgefragt am 25. 1. 2016).

64 Auch eine branchenübergreifende Herausbildung eines Handelsbrauches nur für große Unternehmen – für die der ISO-Standard zugeschnitten scheint – ist abzulehnen, da der Bereich/das Marktsegment, in dem ein Handelsbrauch gilt, objektiv abgrenzbar sein muss. Siehe Kramer/Rauter in Straube, WK § 346 Rz 14 mwN.

Selbst bei Unterstellung der Prämisse, dass sich der ISO-Standard 19600 zu einem Handelsbrauch entwickelt, ist hieraus kein genereller Befolgsdruck für alle Unternehmen ableitbar, ihr CMS in Einklang mit dem Standard zu gestalten. Ein Handelsbrauch dient der Vertragsauslegung oder Vertragsergänzung; wird aber keine Zertifizierung vorgenommen, mangelt es bereits am auszulegenden bzw zu ergänzenden Vertragsverhältnis.

B. ISO 19600 als Verkehrsanschauung?

Der ISO-Standard 19600 könnte hingegen als Verkehrsanschauung allgemeine Geltung entfalten. Eine Verkehrsanschauung gibt eine bestimmte Werthaltung wieder und dient der Konkretisierung von Generalklauseln, wie der „Sorgfalt eines ordentlichen Unternehmers“ gem § 347 UGB.⁶⁵

Der OGH hat sich in Bezug auf Ö-Normen dafür ausgesprochen, dass ein Fachunternehmer verpflichtet ist, sich die notwendigen Kenntnisse, einschließlich der einschlägigen Vorschriften wie Ö-Normen, zu verschaffen.⁶⁶ Die ordentliche Sorgfalt gebietet es demnach, einschlägige Ö-Normen zu berücksichtigen und in Einklang mit diesen zu handeln. Handeln Geschäftsleiter üblicherweise in Einklang mit Ö-Normen, so können diese auch ohne gesetzliche oder vertragliche Verbindlichkeit faktisch gelten; dies, weil Ö-Normen den anerkannten Standard repräsentieren, welcher von einem ordentlichen und gewissenhaften Geschäftsleiter zu wahren ist. Der anerkannte Standard bildet damit den objektiven Sorgfaltsmittelstab. Eine Missachtung der Ö-Norm zieht als Konsequenz einen Sorgfaltsmittelstöß gem § 25 GmbHG bzw § 84 AktG nach sich und kann haftungsgrundend sein. Ö-Normen können folglich *de facto* bindend sein, indem sie den materiellen Sorgfaltsmittelstab determinieren.

Unterwerfen sich Unternehmen freiwillig dem ISO-Standard und erwerben eine Zertifizierung, wird dessen Geltung anerkannt. Geschäftsleiter sind folglich verpflichtet, jene Compliance-Maßnahmen zu ergreifen, die der Zertifizierung zugrunde gelegt wurden. Doch auch ohne Zertifikat könnte der ISO-Standard 19600 einen Befolgsdruck auslösen. Handeln Geschäftsleiter üblicherweise in Anlehnung an den Standard, wird vermutet, dass bei Einhaltung des Standards pflichtkonform gehandelt wurde.⁶⁷ Abweichendes Handeln kann eine Verletzung des objektiven Sorgfaltsmittelstabes bewirken, wenn von einem ordentlichen und gewissenhaften Geschäftsleiter eine Beachtung des ISO-Standards erwartet würde.

Der ISO-Standard 19600 wird hierdurch zur Handlungsmaxime. Werden vergleichbare Unternehmen mit einem Compliance Zertifikat ausgezeichnet bzw wird der ISO-Standard inhaltlich auch ohne Zertifizierung umgesetzt, determiniert dies den üblichen Sorgfaltsmittelstab. Einem gewissenhaften Geschäftsleiter ist es abzuverlangen, den relevanten ISO-Standard zu kennen und entsprechend zu handeln. Wird von einem vergleichbaren Unternehmen üblicherweise eine Compliance-Zertifizierung erlangt, wird eine Zertifizierung *de facto* zwingend. Zumindest ist aber von einem inhaltlichen Gleichlauf auszugehen. MaW sind auch ohne Zertifikat die inhaltlichen Maßstäbe der Zertifizierung zu befolgen. Die Norm ISO 19600 könnte daher als Verkehrsanschauung eine faktische Bindungswirkung entfalten.

65 Kramer/Rauter in Straube, WK § 346 Rz 26; Krejci, Unternehmensrecht⁴ 25.

66 OGH 6. 8. 2015, 2 Ob 223/14d.

67 Scherer/Fruth, Der Einfluss von Standards, Technikklauseln und des „Anerkannten Standes von Wissenschaft und Praxis“ auf Organhaftung und Corporate Governance – am Beispiel der ISO 19600 (2015) Compliance-Management-System, CCZ 2015, 9 (14); vgl auch Strauss/Hermann, Aufsichtsrat aktuell 2014/6, 9.

Dem steht aber – noch – die erst geringe Verbreitung des ISO-Standards 19600 entgegen. Eine CMS-Zertifizierung bildet derzeit die Ausnahme und nicht die Regel. Eine faktische Verpflichtung, eine Zertifizierung vorzunehmen, besteht daher aktuell nicht. Auch eine Pflicht, die inhaltlichen Maßstäbe der Zertifizierung zu befolgen, dh in Einklang mit dem ISO-Standard 19600 zu handeln, stößt an Grenzen: Geschäftsleiter haben ein Organisationsermessen; ein CMS ist immer abhängig von der konkreten Unternehmenssituation zu gestalten. Insb für kleine Einheiten erscheint ein derart umfangreiches CMS, wie vom ISO-Standard vorgegeben, als unverhältnismäßig. Eine Bindung an den ISO-Standard würde Geschäftsleiter in ihrem Organisationsermessen erheblich einschränken. Für große Einheiten scheint eine künftige, faktische Geltung des ISO-Standards 19600 als Verkehrsanschauung hingegen möglich.

C. Geltung über Umwege?

Die ISO 19600 könnten auch über den Umweg der Abschlussprüfung Bindungswirkung erlangen. Gegenstand der Abschlussprüfung bei Kapitalgesellschaften sind gem § 268 UGB der Jahresabschluss und der Lagebericht. In den Lagebericht sind gem § 243a Abs 2 UGB grundsätzlich nur die wichtigsten Merkmale des internen Kontrollsystems und des Risikomanagementsystems in Bezug auf die Rechnungslegung aufzunehmen. Aus einer Gesamtbetrachtung des ÖCGK sind börsennotierte Unternehmen bzw Unternehmen, die sich einer Selbstverpflichtung unterworfen haben, hingegen zur Etablierung eines Risikomanagementsystems auch in nicht-finanziellen Bereichen angehalten. Gem Regel 83 ÖCGK hat der Abschlussprüfer eine Überprüfung der Funktionsfähigkeit des Risikomanagementsystems vorzunehmen. Beurteilungsgegenstand der Abschlussprüfung bilden „die im Unternehmen eingesetzten Systeme und Einrichtungen (Risikomanagementmethoden, Sicherungsstrategien etc, Methoden und Systeme zur Identifikation, Erfassung, Analyse, Bewertung, Kontrollen und Kommunikation der Risiken im Unternehmen etc) [...]. Zur Definition der Begriffe ‚Risiko‘ und ‚Risikomanagement‘ kann dabei auf *internationale Vorbilder und Modelle* zurückgegriffen werden.“⁶⁸ Eine Prüfung durch den Abschlussprüfer setzt voraus, dass eine entsprechende Errichtung und interne Dokumentation des Risikomanagement-Systems besteht, andernfalls die Risikoidentifikation und -beschreibung nicht nachvollzogen werden können.

Der Prüfungsumfang des Abschlussprüfers wird in den Fachgutachten der Kammer der Wirtschaftstreuhänder (KWT) konkretisiert. Werden im Zuge der Prüfung „wesentliche Mängel und Schwächen in den nicht auf die Rechnungslegung bezogenen Bereichen des internen Kontrollsysteins entdeckt“, kann nach Auffassung der KWT die Redepflicht gem § 273 Abs 2 UGB ausgelöst werden. Jedenfalls ist aber die Unternehmensleitung über die aufgedeckten Schwächen zu informieren. Der Abschlussprüfer hat einen Ermessensspielraum, in welcher Form die Berichterstattung über diese Mängel erfolgt.⁶⁹ Die Fachgutachten der KWT enthalten Leitlinien zu verschiedenen Aspekten der Wirtschaftsprüfung und geben nach hA den aktuellen Standard, der an die Prüfungstätigkeit gestellt wird, wieder.⁷⁰ Sie sind grundsätzlich rechtlich unverbindlich. Allerdings

68 Interpretation zu Regel 83 ÖCGK: Hervorhebung durch die Verfasserin.

69 Fachgutachten des Fachsenats für Unternehmensrecht und Revision der KWT über die Durchführung von Abschlussprüfungen, KFS/PG 1, 45 <http://www.kwt.or.at/de/PortalData/2/Resources/downloads/downloadcenter/KFS-PG1.pdf> (abgefragt am 25. 1. 2016); siehe auch Stellungnahme des Fachsenats für Unternehmensrecht und Revision der KWT zu Ausgewählten Fragen zur Redepflicht des Abschlussprüfers gem § 173 Abs 2 und 3 UGB, KFS/PE 18 Rz 12 <http://www.kwt.or.at/de/PortalData/2/Resources/downloads/downloadcenter/KFS-PE18.pdf> (abgefragt am 25. 1. 2016).

70 Reiter, Überprüfung der Prüfer, persaldo 2005/4, 10.

unterwirft § 82 Abs 1 WTBG⁷¹ Wirtschaftstreuhänder der Verpflichtung, in Einklang mit der Richtlinie der KWT zu handeln. Die auf dieser Grundlage ergangene WT-Ausführungsrichtlinie 2003 verpflichtet Wirtschaftstreuhänder gem § 2, „die anerkannten gesetzlichen Regeln, insbesondere die Fachgutachten der Kammer der Wirtschaftstreuhänder, zu beachten“. Wer entgegen dieser Verpflichtung handelt, begeht gem § 120 Z 25 WTBG ein Berufsvergehen, welches disziplinär geahndet werden kann.⁷² Ein sorgfältig handelnder Wirtschaftsprüfer würde in Ausübung seiner Tätigkeit folglich die in den Gutachten niedergelegten Grundsätze achten. Die Einhaltung der üblichen Standards indiziert nach stRsp die Fehlerfreiheit eines Produkts.⁷³ Umgekehrt indiziert dann ein Zu widerhandeln gegen die Gutachten eine Verletzung des aktuellen Prüfungsstandards und damit des objektiven Sorgfaltsmäßigstes des Wirtschaftsprüfers. Hierdurch entfalten die rechtlich unverbindlichen, von einer privaten Institution erlassenen Leitlinien normative Wirkung. Ein sorgfältiger gewissenhafter Abschlussprüfer ist verpflichtet, diese zu befolgen und überprüft demnach auch das Risikomanagementsystem in Bezug auf nicht-finanzielle Risiken, obwohl keine diesbezügliche allgemeine gesetzliche Verpflichtung besteht.

Würde der Abschlussprüfer die ISO 19600 seiner Prüfung als internationales Vorbild zugrunde legen, würden diese zur Beurteilungsgrundlage. Als Konsequenz würde Unternehmen mittelbar auch die Einrichtung eines an der ISO 19600 ausgerichteten CMS auferlegt. Selbst wenn keine faktische Geltung der ISO 19600 aus den anderen erörterten Gründen eintritt, könnten diese damit über die Abschlussprüfung Normativwirkung entfalten.

V. Ergebnis

Eine ISO 19600-Zertifizierung kann für die Geschäftsleitung sowohl haftungserhöhende als auch haftungsmindernde Konsequenzen nach sich ziehen. Auch sorgfaltsmindernde Auswirkungen für Geschäftsführer sind denkbar. Es kann folglich keine generalisierende Aussage darüber getroffen werden, wie sich eine CMS-Zertifizierung tatsächlich auf die Haftung der Gesellschaftsorgane auswirkt.

Auch ohne Zertifizierung könnte eine faktische Geltung des ISO-Standards 19600 als Verkehrsschauung eintreten und damit den objektiven Sorgfaltsmäßigstab beeinflussen. Die Entwicklung eines Handelsbrauches erscheint in Anbetracht der bisher geringen Anzahl an erworbenen Zertifizierungen und der Vielfältigkeit unternehmerischer Tätigkeit zumindest derzeit als nicht wahrscheinlich. Eine faktische Bindungswirkung der ISO 19600 könnte aber auch über den Umweg der Abschlussprüfung eintreten, sofern die ISO 19600 als Prüfungsgrundlage herangezogen werden.

71 Wirtschaftstreuhandberufsgesetz (WTBG) BGBI I 1999/58.

72 *Ladler*, Pflichten des Stiftungsprüfers, PSR 2014, 185 (186 f).

73 OGH 28. 6. 1995, 3 Ob 547/95; 16. 7. 1998, 6 Ob 157/98a; 23. 9. 2004, 6 Ob 73/04k.