universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„Compliance in der Immobilienwirtschaft“

verfasst von / submitted by

Mag. Marie-Christin Gstöttner

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2022/ Vienna 2022

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 361
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Wohn- und Immobilienrecht (LL.M.)
Betreut von / Supervisor:	Univ.-Prof. Dr. Helmut Ofner LL.M.

Inhaltliche Gliederung

Abstract

Wie aus den Medien bekannt, sind österreichische Unternehmen im Immobiliensektor Gegenstand von aktuellen politischen und juristischen Untersuchungen. Im Jahr 2021 sind sowohl Strafen verhängt als auch Ermittlungsverfahren gegen namhafte Vertreter der Bau- und Immobilienbranche eingeleitet worden. Dies vor dem Hintergrund unlauterer Verhaltensweisen der Unternehmen (Preisabsprachen bei Ausschreibungen etc.) sowie unzulässiger Beeinflussung (Korruptionsstraftatbestände). Auch wenn in diesen medial kolportierten Fällen nicht immer Strafen verhängt werden, ist in jedem Fall ein Reputationsschaden für die Betroffenen gegeben. Am Beispiel der zuletzt seitens der Bundeswettbewerbsbehörde verhängten Strafen gegen an einem Baukartell beteiligte Bau- und Immobilienunternehmen, hat die Behörde bei der Strafzumessung gegenüber eines der beteiligten Unternehmen als strafmildernd angeführt, dass dieses ein sogenanntes Compliance Management System eingeführt hat.

In der vorliegenden Arbeit soll daher vorrangig der Frage nachgegangen werden, was ein Compliance-Management-System ist und welche Auswirkungen die Einführung eines solchen im Unternehmen hat. Abgesehen von einzelnen Bereichen, z.B. der Geldwäscheprävention, ist der Immobiliensektor – im Gegensatz zur Banken, Versicherungs- oder Pharmabranche - grundsätzlich kein Bereich, welcher strengen regulatorischen (Compliance-) Bestimmungen unterliegt. Es soll daher die Frage nach der Notwendigkeit der Einführung eines Compliance-Management-Systems in Immobilienunternehmen herausgearbeitet werden.

Vorwort - Compliance im Recht

Compliance wird oftmals beschrieben als Einhaltung von Regeln in Form von Recht und Gesetz. Compliance wird dabei übersetzt mit „Regelkonformität“ im weitesten Sinn. Im Hinblick auf „Corporate Compliance“, also Compliance in Unternehmen, sind damit alle Maßnahmen gemeint, welche ein regelkonformes Verhalten im Unternehmen gewährleisten sollen. Regelkonformität in diesem Kontext bedeutet dabei, die Organe und Mitarbeiter eines Unternehmens beachten sämtliche auf sie anwendbare Regeln und verhalten sich entsprechend diesen Regeln. Anwendbare Regeln sind jedenfalls die Normen der allgemeinen Rechtsordnung, zusätzlich – wie in vielen Unternehmen längst gelebte Praxis – auch selbst auferlegte Verhaltensregeln, typischerweise niedergeschrieben in Verhaltenskodizes und Compliance Richtlinien. Verhaltenskodizes legen typischerweise

die unternehmensinternen Verhaltensgrundsätze fest, welche die rechtlichen Anforderungen an das Unternehmen und seine Mitarbeiter darstellen. Die Herausforderung an der Compliance-Arbeit besteht an der Interpretation und Implementierung dieser Verhaltensanforderungen in die Unternehmensabläufe mit dem Ziel der Verhinderung und Aufdeckung von bewussten und unbewussten Regelverstößen. Dies erfolgt typischerweise durch die Implementierung eines Compliance-Management-Systems, welches verschiedene Maßnahmen enthält, um die unternehmensintern verankerten Compliance-Grundsätze und Prinzipien umzusetzen. Compliance ist, meines Erachtens, mit dem kodifizierten Recht beziehungsweise dem normativen Rechtssystem insofern verbunden, als Compliance dazu dient, Verstöße gegen Gesetze und rechtliche Bestimmungen sowie intern festgelegte Handlungsgrundsätze zu verhindern beziehungsweise aufzudecken und nicht-rechtskonformen Verhaltensweisen vorzubeugen. Dies mit dem Ziel, das Unternehmen, die Organe und die Mitarbeiter zu schützen.[1]

[1] *Jaufer* in SWK 19/2011, W 41

I. Eingliederung und Bedeutung von Compliance in der Immobilienwirtschaft

Wie aus Medien bekannt, ist es in jüngerer Zeit vermehrt zu (Ermittlungs-)verfahren beziehungsweise Strafen gegen Bau- und Immobilienunternehmen gekommen – aufgrund von „Non-Compliance" der involvierten Unternehmen im Wirtschaftsleben. Dies vor dem Hintergrund unlauterer Verhaltensweisen (kartellrechtliche Preisabsprachen etc.) sowie unzulässiger Beeinflussung durch die involvierten Unternehmen (Korruptionsstraftatbestände). Kartell- und Korruptionsrecht sind Rechtsgebiete, die klassischerweise unter dem Begriff „Compliance" subsumiert werden.

Diese Entwicklung zeigt die zunehmende Bedeutung von Compliance im Allgemeinen sowie im speziellen in der Privatwirtschaft und im Immobiliensektor. Im Gegensatz zur Banken-, Versicherungs- oder Pharmabranche, ist die Immobilienwirtschaft grundsätzlich kein Bereich, welcher strengen regulatorischen (Compliance-) Bestimmungen unterliegt. Es bestehen lediglich auf bestimmte Materien beschränkte Compliance-Pflichten, wie z.B. im Bereich der Geldwäscheprävention und Terrorismusbekämpfung, der zufolge Immobilienmakler, Rechtsanwälte und Notare gewissen Sorgfaltsverpflichtungen (so etwa dem Durchführen einer Risikoanalyse), nachkommen müssen. Auch in Vergabeverfahren finden sich unter den im Gesetz angeführten Grundsätzen ausdrückliche Compliance-Verpflichtungen. So haben gemäß § 26 BVergG öffentliche Auftraggeber geeignete Maßnahmen zu treffen, um Interessenkonflikte wirksam zu verhindern, aufzudecken und zu beheben. Der im Gesetz festgelegte Grundsatz dient dazu, Wettbewerbsverzerrungen zu vermeiden und eine Gleichbehandlung aller Unternehmer zu gewährleisten.

Neben der Analyse einzelner materiellrechtlicher Compliance-Verpflichtungen soll in der vorliegenden Arbeit insbesondere auch auf die (gesetzlichen) Grundlagen und die Frage nach der rechtlichen Verpflichtung beziehungsweise der Notwendigkeit der Einführung eines sogenannten Compliance-Management-Systems, sohin eines unternehmensweiten Systems mit dem primären Ziel, Fälle von „Non-Compliance" zu verhindern, eingegangen werden.

Es werden dazu in der vorliegenden Arbeit die relevanten Bestimmungen in den österreichischen Gesetzen beleuchtet, welche sich vor allem im Gesellschaftsrecht, Strafrecht (Verbandsverantwortlichkeit), aber auch im Verwaltungsrecht (Verwaltungsstrafrecht) finden.

Zur Erörterung der Notwendigkeit und der Auswirkungen der Einführung eines Compliance-Systems wird am Beispiel der zuletzt seitens des Bundeswettbewerbsbehörde beantragten und des Kartellgerichts verhängten Strafen in Millionenhöhe – darunter die bisher höchste Kartellstrafe in Österreich - gegen diverse Unternehmen in der Bauwirtschaft, welche jahrzehntelang Preise bei Ausschreibungen abgesprochen haben, und in welchem das Kartellgericht gegen eines der involvierten Unternehmen eine deutlich mildere Strafe ausgesprochen hat, ersichtlich, dass Compliance-Management-Systeme nicht nur als Präventivmaßnahme, sondern auch als potentieller Strafmilderungsgrund bei der Strafbemessung von Relevanz sind.

Die Berücksichtigung von Compliance-Anstrengungen und Programmen – auch als Teil der Strafbemessung - findet sich vorwiegend in den Bereichen des Kartellrechts und des Korruptionsrechts. So ist die strafmildernde Wirkung von Compliance-Systemen in Entscheidungen des Kartellgerichts bestätigt worden[2]. In Deutschland ist Compliance als zu berücksichtigender Umstand bei der (kartellrechtlichen) Strafbemessung seit 2021 sogar gesetzlich verankert (sogenannte „Compliance-Defence“). Im Korruptionsrecht ist im anglo-amerikanischem Rechtsraum, insbesondere nach der Rechtsordnung von Großbritannien (UK Bribery Act), die Möglichkeit der Haftungsmilderung durch Compliance-Management-Systeme anerkannt.

In dem angesprochenen Verfahren gegen führende österreichische Bauunternehmen, hat die Bundeswettbewerbsbehörde beim Antragstellen auf Verhängung einer Geldstrafe folgendes festgehalten: *„STRABAG kooperierte kontinuierlich und umfassend im Rahmen des Kronzeugenprogrammes. Zudem wurde durch STRABAG ein zertifiziertes Compliance-System in Verbindung mit einem neuartigen Monitoring-System eingeführt, um zukünftige Zuwiderhandlungen gegen das Kartellverbot hintanzuhalten. STRABAG hat im Rahmen der Kooperation mit der BWB, unter Einbindung des Bundeskartellanwalts, auch ein Anerkenntnis für das kartellgerichtliche Verfahren abgegeben. Vor diesem Hintergrund hat die BWB eine geminderte Geldbuße beantragt*. “[3]

Aus den Erwägungen der Bundeswettbewerbsbehörde sind zwei Punkte bemerkenswert: Zum einen wird zum ersten Mal als unmittelbare Folge des Verfahrens bei einem der involvierten Unternehmen ein sogenanntes Compliance-Monitoring-System eingesetzt.

[2] Vgl. dazu etwa 26 Kt 105/13, 25 Kt 76/14

[3] Homepage BWB; Artikel „Antrag auf Verhängung einer Geldbuße gegen STRABAG“, 14.7.2021, BWB stellt Antrag auf Verhängung einer Geldbuße gegen STRABAG: BWB Bundeswettbewerbsbehörde

Bei diesem nach US-amerikanischem Vorbild bekannten System wird eine Stelle im Unternehmen eingerichtet, besetzt durch eine seitens einer unabhängigen dritten Stelle – im konkreten Fall durch eine Compliance-Zertifizierungsstelle - vorgeschlagene unternehmensfremde Person. Das Compliance-Monitoring-System dient dem primären Zweck, die Effektivität des bestehenden betrieblichen Compliance-Management-Systems zu prüfen und zur kontinuierlichen Verbesserung ebendiesem beizutragen.

Des Weiteren hebt die Bundeswettbewerbsbehörde ausdrücklich das Bestehen eines zertifizierten Compliance-Management-Systems hervor. Jene beiden Punkte – zertifiziertes Compliance-System in Verbindung mit einem Monitoring-System – werden von der Bundeswettbewerbsbehörde, neben der Kronzeugeneigenschaft und dem abgegebenen Anerkenntnis des Unternehmens für das kartellgerichtliche Verfahren, als Umstände angeführt, welche zur milderen Strafe geführt haben.

Aus den Erwägungen der Behörde ergibt sich der Stellenwert von Compliance-Maßnahmen, insbesondere der Einführung und der laufenden Überprüfung und Anpassung von Compliance-Management-Systemen.

Die Bedeutung von Compliance, die Darstellung und Analyse der bestehenden Compliance-Regelungen in immobilienrelevanten Gesetzen sowie die (gesetzlichen) Grundlagen für die Einführung von Compliance-Management-Systemen in Bau- und Immobilienunternehmen, sowie die Auswirkungen der Einführung von Compliance-Programmen, sollen gleichsam den Schwerpunkt der vorliegenden Arbeit darstellen.

A. Definition des Begriffs „Compliance“ und „Compliance-Organisation“

Im österreichischen Recht existiert keine gesetzliche Definition des Begriffs beziehungsweise des Themenfeldes „Compliance“. Es besteht kein branchenübergreifendes Regelwerk, welches den Begriff „Compliance“ definiert beziehungsweise verwendet.[4]

Der englische Begriff– „to comply“ – kann übersetzt werden mit „(Regeln) entsprechen“.

Der Prüfungsstandard IDW PS 980 des Instituts der deutschen Wirtschaftsprüfer, welcher als einer der ersten Compliance Prüfstandards etabliert und bis heute Gültigkeit hat, enthält folgende Definition: „*Unter Compliance ist die Einhaltung von Regeln zu verstehen (gesetzliche Bestimmungen und unternehmensinterne Richtlinien)“.* Ähnlich die Definition

[4] *Petsche/Mair*, Handbuch Compliance³ 29

im deutschen Corporate Governance Kodex: „*Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzerneinheiten hin (Compliance)*“.[5] Der deutsche Verein EBM-Wertemanagement Bau e.V. definiert Compliance als „*die Erfüllung und Einhaltung von Gesetzen, Verordnungen, sonstigen Rechtsvorschriften sowie Richtlinien und Verhaltensregeln, also aller normativen Vorgaben eines Unternehmens, unabhängig davon, ob sich eine Vorgabe aus zwingendem Recht oder einer freiwilligen Selbstverpflichtung ergibt.“* In Kurzform könne Compliance „*als Einhaltung aller maßgeblichen Rechtsvorschriften und unternehmensinternen Verhaltensstandards*“ bezeichnet werden.[6]

Als Ausgangspunkt von Corporate-Compliance-Systemen, sohin Compliance Regelwerken in Unternehmen, können die in den 1960er Jahren strafrechtlich verfolgten amerikanischen Unternehmen der Elektroindustrie wegen wettbewerbsrechtlicher Verstöße und die daraufhin in den betroffenen Unternehmen implementierten Maßnahmen zur Entwicklung von Präventivmaßnahmen zur Vermeidung von Kartellabsprachen, gesehen werden.

Wie von *Kalss* dargestellt, hat sich aus diesen Erfahrungen das Verständnis von Compliance derart etabliert, dass darunter weitläufig die Sicherstellung gesetzeskonformen Verhaltens im Unternehmen durch entsprechende organisatorische Maßnahmen verstanden wird.[7] Des Weiteren führt jene aus, dass sich aus der Leitungspflicht der jeweiligen Unternehmensführung die Sicherstellung rechtskonformen Verhaltens im Unternehmen ergibt. Während dabei die eigene Einhaltung (*Anm.: Einhaltung durch die Leitungsorgane*) die Compliance-Pflicht im engeren Sinn ist, ist die Compliance-Organisationspflicht die Sicherstellung der Einhaltung durch die anderen.[8]

Die „Compliance“ hat sich zunächst im Bankwesen sowie im medizinischen Bereich etabliert. Der Begriff der „Corporate Compliance“, also Compliance in wenig regulierten Branchen der Industrie, hat sich über die letzten ungefähr 15 Jahre entwickelt. Spannend sind die unterschiedlichen Themenbereiche, welche – brachen- und unternehmensspezifisch – unter „Corporate Compliance“ zusammengefasst werden. Dies kann von „klassischen“ Compliance Themen, wie Korruptions- und

[5] *Erwin-Fierel-Giedenbacher/Karin Mair* in *Peter Lewisch*, Zauberwort Compliance? 16
[6] Webseite des EMB: EMB_25_Jahre_Broschuere.pdf (emb-werte.com) 9
[7] *Kalss* in *Kalss/ Torggler*, Beiträge zum 4. Unternehmensrechtstag (2016) 2f
[8] *Kalss* in *Kalss/ Torggler*, Beiträge zum 4. Unternehmensrechtstag (2016) 7

Geldwäschebekämpfung, zu sehr spezifischen Themengebieten, wie etwa Umwelt-Compliance, Produkt-Compliance, reichen.

Nach der Definition des Basel Committee sowie des Deutschen Corporate Governance Kodex umfasst Compliance nicht nur alle anwendbaren Gesetze, sondern auch freiwillige Verhaltensvorschriften, sogenanntes „soft law".

Verschiedene Experten- und Literaturmeinungen sehen hinsichtlich des Compliance-Begriffs neben der juristischen Dimension auch eine starke moralische und ethische Komponente. Diese Dimensionen werden häufig unter dem Stichwort „Integrity" beziehungsweise „Werte-Management" zusammengefasst. Damit im Zusammenhang steht auch die „Corporate Social Responsibility". Dieser Bereich wird mit den jüngsten Entwicklungen im Bereich ESG (Ethics Social Governance) immer relevanter.[9]

Der Anreicherung des Begriffs um ethische Komponenten entspricht der anglo-amerikanischen Betrachtungsweise. So stellen beispielsweise die US Sentencing Guidelines wesentlich auf ethische Aspekte bei der Compliance-Arbeit ab.

In Deutschland wird der Begriff Compliance allgemein stärker mit Wertemanagement assoziiert.

An dieser Stelle soll auch der Zusammenhang zwischen Compliance und Corporate Governance dargestellt werden. So dient der Österreichische Corporate Governance Kodex (ÖCGK) als Maßstab für gute Unternehmensführung und Unternehmenskontrolle. Er wendet sich an alle österreichischen börsenotierten Unternehmen und erlangt durch freiwillige Selbstverpflichtung Geltung. Der Begriff der Corporate Governance ist im Verhältnis zur Compliance weiter, weil er alle Regelungen und anerkannten Standards sorgfältiger Unternehmensführung umfasst. Wie von *Napokoj* dargestellt, kann Compliance als Teil oder wesentlicher Standard einer guten Corporate Governance gesehen werden, zumal anzunehmen ist, eine gute Unternehmensführung umfasse eine dem Unternehmen angepasste Compliance-Organisation.

Einen weiteren Unterschied zwischen Compliance und Corporate Governance sieht *Napokoj* in der Perspektive. So sei bei Corporate Governance die Sichtweise des Regulierers prägend, bei Compliance erfolge die Betrachtungsweise aus dem Blickwinkel der Regulierten, sohin der Unternehmen. Auch bei Zielen, Zwecken und Hintergründen

[9] *E. Napokoj* in *Napokoj*, Risikominimierung Rz 5

gebe es, entsprechend *Napokoj*, Unterschiede. So stehe bei dem ÖCGK die Förderung des Vertrauens von Investoren als auch Transparenz im Vordergrund, Compliance ziele allerdings auf den Schutz des Unternehmens, der Organe sowie der Mitarbeiter ab.[10] Dieser Rechtsmeinung ist zu folgen, Compliance etabliert sich allerdings ebenfalls zunehmend als vertrauensfördernde und für Investoren (vor allem im internationalen Umfeld) unabdingbare Voraussetzung, weshalb sich meines Erachtens die beiden Begriffe immer mehr aneinander annähern.

B. Ursprung und relevante Entwicklungen in der Immobilienwirtschaft

Gewissermaßen als „Geburtsstunde der Compliance“ in der Immobilienwirtschaft ist die Gründung der Compliance-Initiative der deutschen Bauwirtschaft Ende der Neunzigerjahre zu sehen. Diese ist gegründet worden nach Bekanntwerden von Preis- und Submissionsabsprachen sowie Korruption in der Auftragsakquisition durch Bau- und Immobilienunternehmen. In dieser Zeit entstanden und bis heute aktiv ist der Verein Ethikmanagement in der Bauwirtschaft e.V. (heute: EMB Wertemanagement Bau e.V.),[11] welcher sich federführend mit der Entwicklung von Compliance-Strategien und umfassenden wertebasierten Managementkonzepten für deutsche Bauunternehmen beschäftigt. So erhebt der Verein den Anspruch, alle Unternehmen, die sich dem EMB-Wertemanagement Bau anschließen und die von diesem festgelegten Punkte erfüllen, signalisieren und dokumentieren, jene verhalten sich gegenüber aller am Bau Beteiligten rechtstreu, integer und fair[12]. Das EBM Wertemanagement Bau besteht satzungsgemäß aus vier zentralen Elementen:

- Kodifizierung (Ethikkodex oder sonstiges gleichwertiges Dokument, welches die Grundwerte des Unternehmens schriftlich festlegt)

- Implementierung (Entwicklung von unternehmensspezifischen Verhaltensstandards)

- Kontrolle (Umsetzung der Grundwerteerklärung und der Verhaltensstandards im Unternehmensalltag wird in einem turnusmäßig durchgeführten externen Auditverfahren überprüft)

[10] *E. Napokoj* in *Napokoj*, Risikominimierung Rz 9
[11] Interview mit Prof. Dr. Grüninger, “Wir müssen herausfinden, worauf es ankommt“, Compliance Praxis 4/2020, 8-11
[12] Satzung des EMB, Webseite des EMB: 20191007_Satzung_und_Richtlinien.pdf (emb-werte.com)

- Organisation (Firmeninhaber oder Geschäftsleitung hat Vorbildfunktion und trägt die Verantwortung für das Wertemanagementsystem sowie dessen umfassende und ernsthafte Umsetzung im Unternehmen).[13]

Der Vergabesenat des OLG Brandenburg hat dazu entschieden, die Einführung eines Wertemanagements und der Beitritt zum EMB-Trägerverein seien wirkungsvolle Maßnahmen, um die vergaberechtliche Zuverlässigkeit eines Auftragsbewerbers bei der Vergabe eines öffentlichen Bauauftrags wiederherzustellen. So hieß es in der Entscheidung dazu: „*Schließlich durften Auftraggeber und Vergabekammer die weiteren von dem Bauunternehmen ergriffenen präventiven Maßnahmen, nämlich… die Einführung eines Wertemanagements in der Unternehmensgruppe und den Beitritt zum ‚Ethikmanagement der Bauwirtschaft e.V.' als geeignet ansehen, eine Wiederholung der Verfehlungen zu erschweren bzw. unmöglich zu machen."*

In den letzten 10 Jahren haben unterschiedliche deutsche Konzerne und Unternehmensgruppen verbindlich mitgeteilt, dass sie gegenüber auditierten EBM-Mitgliedsfirmen die Compliance-Anforderungen als vollumfänglich erfüllt ansehen. So hat unter anderem der Siemens-Konzern festgehalten, bei der Vergabe von Aufträgen gegenüber auditierten EBM-Mitgliedsfirmen, die eine gültige EBM-Auditurkunde vorlegen, auf anderweitig beizubringende Nachweise zu verzichten. Mittlerweile haben sich weitere namhafte Konzerne der deutschen Wirtschaft, wie etwa die Deutsche Bahn als auch die Flughafen München GmbH, für diese Vorgehensweise entschieden. [14]

Des Weiteren erwähnenswert im deutschen Rechtsraum ist das Institut für Corporate Governance in der Immobilienwirtschaft (ICG), welches sich für werteorientierte, nachhaltige Unternehmensführung einsetzt. Bei dem seit 2002 bestehenden Institut handelt es sich um ein Think-thank für Governance, Transparenz und Integrität, welche Auditierungen und Zertifizierungen durchführt.

So hat das ICG unter anderem auch ein Zertifizierungssystem für Compliance-Management eingerichtet. Basis dafür ist ein „Pflichtenheft", in welches aktuelle Prüfstandards eingeflossen sind, allen voran der Prüfstandard IDW PS 980. Das auf ICG-

[13] Webseite des EMB: EMB_25_Jahre_Broschuere.pdf (emb-werte.com) 10
[14] Webseite des EMB: EMB_25_Jahre_Broschuere.pdf (emb-werte.com) 12

Prinzipien basierende Compliance-System wird im Prüfstandard IDW PS 980 als Branchenstandard empfohlen. [15]

Das Institut für Corporate Governance in der deutschen Immobilienwirtschaft führt jährlich – in Kooperation mit der KPMG Wirtschaftsprüfungsgesellschaft – eine Governance-Studie für die Immobilienwirtschaft durch. Der zuletzt veröffentlichte Bericht von November 2021 widmet sich der Zunahme an einschlägig relevanten Bestimmungen, vor allem im Hinblick auf ESG (Environmental, Social, Governance) als auch dem in Deutschland im Frühjahr 2021 ausgerollten Finanzintegritätsstärkungsgesetz, welches bestimmte Governance-Verpflichtungen für börsennotierte Unternehmen vorsieht.

Der Governance-Bericht unterscheidet kategorisch in vier Bereiche:

(1) Interne Revision
(2) Internes Kontrollsystem
(3) Risikomanagement
(4) Compliance

Die durchgeführte Studie kommt zu dem Schluss, dass die genannten vier Governance-Funktionen, welche vor allem eine Beratungs- und Überwachungsfunktion haben, bei den an den Studien beteiligten Unternehmen mehrheitlich vorhanden sind. Dementsprechend kommt die Studie zum Schluss, die Bedeutung guter Corporate Governance würde auch in der Immobilienbranche anerkannt werden.[16]

Interessante Erkenntnis aus dieser Studie ist unter anderem die Einstufung der relevanten Compliance-Risiken im eigenen Unternehmen, wonach der Datenschutz beziehungsweise die IT-Sicherheit als wichtigstes Compliance Risiko gesehen wird, gefolgt von der Betrugs- und Gelwäscheprävention. Des Weiteren sind Korruptionsprävention und Interessenkonflikte als Risiken genannt worden. Der Großteil der befragten Unternehmen hat eine dokumentierte Risikoanalyse. Als Hauptaspekte der Compliance-Funktion sehen die beteiligten Unternehmen sowohl eine Beratungs- als auch eine Überwachungsfunktion.[17]

[15] Webseite des ICG: Homepage – Institut für Corporate Governance (icg-institut.de)
[16] Governance-Studie für die Immobilienwirtschaft 2021 (Governance-Studie für die Immobilienwirtschaft 2021 (icg-institut.de), 7
[17] Governance-Studie für die Immobilienwirtschaft 2021 (Governance-Studie für die Immobilienwirtschaft 2021 (icg-institut.de), 13f

C. Compliance-Organisation: Bestimmungen und Entwicklungen in Österreich

Wie einleitend dargelegt, hat die Intensität an einschlägigen (Ermittlungs-)verfahren aufgrund von Non-Compliance der betroffenen Unternehmen über die letzten Jahre zugenommen und hat gleichzeitig die Aktualität von Compliance beziehungsweise die Einführung und Weiterentwicklung von betriebsinternen Compliance-Management-Systemen zugenommen.

Eine generelle Verpflichtung zur Implementierung einer Compliance-Organisation wird vom österreichischen Gesetzgeber nicht explizit vorgeschrieben – Ausnahmen stellen die einschlägigen, branchenspezifische Gesetze dar, so etwa das FM-GWG als auch die wertpapierrechtlichen Bestimmungen[18]. So heißt es in § 29 Wertpapieraufsichtsgesetz: „*Ein Rechtsträger hat durch Festlegung angemessener Strategien und Verfahren dafür zu sorgen, dass er selbst, seine Geschäftsleitung, Beschäftigten und vertraglich gebundenen Vermittler den Verpflichtungen dieses Bundesgesetzes sowie den organisatorischen Anforderungen und Ausübungsbedingungen des Kapitel II und des Kapitel III der delegierten Verordnung (EU) 2017/565 dieser Personen nachkommen („Compliance“)*." Hier wird „Compliance" primär verwendet, um auf die Notwendigkeit der Einführung angemessener Strategien und Verfahren, zwecks Regeleinhaltung der dort angeführten Personengruppen – Geschäftsleitung, Beschäftigte und vertraglich gebundene Vermittler - hinzuweisen.

Ebenfalls eine ausdrückliche Erwähnung der Compliance-Funktion findet sich in § 117 Versicherungsaufsichtsgesetz (VAG), wonach ein internes Kontrollsystem, neben einem Verwaltungs- und Rechnungslegungsverfahren sowie einem internen Kontrollrahmen, zwei Elemente aufzählt, welche klassische Compliance-Materien beinhalten, nämlich einem angemessenen Melde- und Berichtswesen sowie einer Compliance-Funktion.

Des Weiteren sehen einschlägige standesrechtliche Regelungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung vor, dass bei Erfüllung der dort genannten Voraussetzungen die Bestellung eines Compliance-Beauftragten zu erfolgen hat.

Als mögliche Anknüpfungspunkte für die Einführung von Compliance-Management-Systemen werden in der Literatur folgende gesetzliche Grundlagen herangezogen:

[18] *Petsche/Mair*, Handbuch Compliance³ 29

- Gesellschaftsrecht (Allgemeine Sorgfaltspflichten - § 84 AktG und § 25 GmbHG sowie Pflichten zur Einführung eines internen Kontrollsystems durch die obersten Leitungsorgane - § 82 AktG und § 22 Abs. 1 GmbHG)
- Strafrecht (Verbandsverantwortlichkeitsgesetz, insb. Mitarbeiterstraftat, § 5 VbVG)
- Verwaltungsrecht (Verwaltungsstrafrecht - § 9 VStG)

Detailliertere Ausführungen dazu finden sich unter Punkt IV.

Ergänzend zu den Verpflichtungen, welche sich aus den einschlägigen gesetzlichen Bestimmungen ergeben, kann die Entscheidung, ein innerbetriebliches Compliance-Management-System einzuführen, auch das Ergebnis einer durchgeführten Risiko-Analyse sein. Dazu näheres unter Kapitel IV. F.

D. Aktuelle Entwicklungen in Deutschland

Im Oktober 2021 hat das deutsche Bundeskartellamt aktualisierte Leitlinien zur Bußgeldbemessung in Kartellordnungswidrigkeitsverfahren herausgegeben. In den Erläuterungen zu den Leitlinien für die Bußgeldzumessung wird auf die sogenannte „Vortat-Compliance“ sowie die „Nachtat-Compliance“ eingegangen und die Compliance Maßnahmen als mildernd berücksichtigt.[19] So heißt es in dem Leitfaden zur „Vortat-Compliance“: „*Ein berücksichtigungsfähiger Faktor* (Anm.: Bezüglich der Zumessungskritierien im Hinblick auf den Bußgeldrahmen) *sind Vorkehrungen zur Vermeidung und Aufdeckung von entsprechenden Zuwiderhandlungen (Compliance). Art und Umfang von erforderlichen Vorkehrungen hängen vom jeweiligen Einzelfall ab und dabei insbesondere von Art, Größe und Organisation eines Unternehmens, den zu beachtenden Vorschriften sowie dem Risiko ihrer Verletzung. Mildernd kann zum einen berücksichtigt werden, dass im Unternehmen bereits zur Tatzeit alle objektiv erforderlichen Vorkehrungen ergriffen worden sind, um kartellrechtliche Zuwiderhandlungen wirksam zu verhindern (Vortat-Compliance). Eine Wirksamkeit von Vortat-Compliance ist in der Regel dann anzunehmen, wenn die getroffenen Vorkehrungen zur Aufdeckung und umgehenden Anzeige der Zuwiderhandlung geführt haben. (….)*

[19] Webseite des deutschen Bundeskartellamt - Bußgeldleitlinien_Oktober2021.pdf;jsessionid=E2C2AC53FEB7B5F533F224B984DF11E8.1_cid362 (bundeskartellamt.de)

Des Weiteren ergibt sich aus dem Leitfaden auch, dass gewisse, nach einem „Non-Compliance Fall“ gesetzte Aktivitäten – unter dem Begriff „Nachtat-Compliance“ zusammengefasst – als mildernd berücksichtigt werden können. Die nach der Tat getroffenen Vorkehrungen müssen zur effektiven Vermeidung und Aufdeckung von entsprechenden Zuwiderhandlungen im Rahmen einer Gesamtbetrachtung geeignet sein.

Eine Milderung zieht das Bundeskartellamt insbesondere in Betracht, *„wenn das Unternehmen überzeugend die ergriffenen Vorkehrungen zur wirkungsvollen Vermeidung künftiger vergleichbarer Verstöße darlegt und ein Bekenntnis zu rechtskonformem Handeln klar erkennbar ist. Ein wichtiges Indiz für die Ernsthaftigkeit von Nachtat-Compliance ist zum einen, dass ein Unternehmen bei der Aufklärung der Tat aktiv kooperiert. Zum anderen fließt auch das Bemühen, den Schaden wiedergutzumachen, in diese Beurteilung der Ernsthaftigkeit mit ein. Aktive Kooperation bei der Aufklärung und das Bemühen um Schadenswiedergutmachung sind zugleich auch eigenständig zu bewertende Aspekte des positiven Nachtatverhaltens (Doppelfunktion“*.[20]

Im deutschen Gesetz gegen Wettbewerbsbeschränkungen (GWB) ist im Rahmen der 10. GWB Novelle („Digitalisierungsnovelle“) mit Wirkung zum 19.1.2021 bei der Festsetzung der Geldbuße, welche gegen Unternehmen wegen Verstößen gegen das Kartellverbot oder das Missbrauchsverbot, festgesetzt werden, als abzuwägende Umstände folgendes festgeschrieben worden:

§ 81d Abs. 1 Z 4 GWB: „*vorausgegangene Zuwiderhandlungen des Unternehmens sowie vor der Zuwiderhandlung getroffene, angemessene und wirksame Vorkehrungen zur Vermeidung und Aufdeckung von Zuwiderhandlungen*“

§ 81 d Abs. 1 Z 5 GWB: „*das Bemühen des Unternehmens, die Zuwiderhandlung aufzudecken und den Schaden wiedergutzumachen sowie nach der Zuwiderhandlung getroffene Vorkehrungen zur Vermeidung und Aufdeckung von Zuwiderhandlungen. “*[21]

Mit der GWB-Digitalisierungsnovelle erfolgte eine gesetzliche Klarstellung, wonach getroffene Compliance Maßnahmen das Kartellbußgeld reduzieren können. Für die Zumessung der konkreten Geldbuße sollen die in § 81d GWB verankerten Kriterien eine

[20] Webseite des deutschen Bundeskartellamt - Leitlinien für die Bußgeldzumessung in Kartellordnungswidrigkeiten (Bußgeldleitlinien_Oktober2021.pdf (bundeskartellamt.de))
[21] *Schultze* in *Schultze*, Compliance-Handbuch Kartellrecht, 2. Auflage (2021), Teil A, RZ 1

einheitliche Orientierungshilfe geben. Durch die gesetzliche Festschreibung von „Vortat-Compliance“ und „Nachtat-Compliance“ als mögliche Strafmilderungsgründe einerseits als auch durch die eindeutigen Ausführungen im Leitfaden zur Bußgeldbemessung sind Grundlagen geschaffen worden, um die Wichtigkeit effektiver und wirksamer Compliance-Management-Systeme hervorzuheben und solche in Unternehmen zu verankern.[22]

Ebenfalls erwähnenswert ist der vorliegende Entwurf zum deutschen Gesetz zur Sanktionierung von verbandsbezogenen Straftaten (kurz: Verbandssanktionengesetz). Der Entwurf sieht Geldbußen für Unternehmen bei unternehmensbezogenen Gesetzesverstößen vor. Hervorzuheben ist bei dem Entwurf besonders der hohe Stellenwert, welcher effektiven Compliance-Management-Systemen als Milderungsgrund zukommt. Umgekehrt droht bei Vernachlässigung von Compliance im Unternehmen eine Strafverschärfung. Der Gesetzesentwurf schafft damit Anreize für die Implementierung von Compliance-Maßnahmen.[23]

Das Verbandssanktionengesetz würde eine deutliche Weiterentwicklung im Vergleich zum bestehenden Ordnungswidrigkeitengesetz bedeuten, welches nach dem Opportunitätsprinzip aufgebaut ist, wonach es im Ermessen der Strafverfolgungsbehörden liegt, ob Unternehmen für verbandsbezogene Straftaten geahndet werden.

Das Gesetzesvorhaben ist zum Zeitpunkt des Verfassens der Arbeit von der deutschen Regierung nicht weiter behandelt worden.

E. Internationale Einflüsse

Wie in der Literatur richtigerweise herausgearbeitet, resultiert die internationale Zunahme von Compliance-Programmen (auch) aus dem Umstand, dass die in den Sitzstaaten internationaler Konzerne geltenden Regelungen und die darauf aufgebauten Compliance-Anforderungen und Programme auf andere Staaten, in welchen Tochtergesellschaften beziehungsweise Zweigniederlassungen bestehen, übertragen werden. Dies in zweifacher Hinsicht: Zum einen übertragen internationale Konzerne ihre „Heimatstandards“ beziehungsweise die Standards jenes Landes, in welchem die strengsten Compliance-Anforderungen gelten. Zum anderen werden die eigenen Compliance-Standards

[22] Dazu *Strammwitz* in Compliance-Berater: „Kehrtwende: 10. GWB-Novelle erkennt „Compliance-Defence“ im Kartellbußgeld an“

[23] *Eckel/Lörincz*: „Deutsches Verbandssanktionengesetz: Strafmilderung durch Compliance und Koordination“, Compliance Praxis 4/2020, 36-38

Geschäftspartnern beziehungsweise Zielunternehmen auferlegt. Dies ist besonders oft der Fall bei US-amerikanischen Mutterkonzernen.[24]

Als internationale Regelwerke sind vor allem die strengen Anti-Korruptionsbestimmungen des US-amerikanischen Foreign Corrupt Practices Act („FCPA") und des UK Bribery Act („UKBA") zu nennen, welche spezifische Regelungen enthalten, um kriminellen Verhaltensweisen betriebsintern vorzubeugen. Die beiden Gesetze kennzeichnen sich durch einen sehr weiten Anwendungsbereich sowie durch die teilweise extraterritoriale Anwendbarkeit aus.

Der UK Bribery Act gilt zurecht als das strengste Anti-Korruptionsgesetz weltweit, welches von Unternehmen im Rahmen der Corporate Compliance klare Anti-Korruptions- und Risk Assessment-Maßnahmen einfordert. Dies betrifft auch alle österreichischen Unternehmen, die in irgendeiner Form geschäftlich im Vereinigten Königreich aktiv sind.[25]

In den USA sind neben dem Foreign Corrupt Practices Act vor allem die US Sentencing Guidelines relevant. Die US Sentencing Guidelines ziehen für die Berechnungsgrundlage für das konkrete Strafmaß in Betracht, ob ein Unternehmen ein effektives Programm zur Verhinderung und Aufdeckung von Rechtsverletzungen („*effective programme to prevent and detect violations of law*") eingerichtet hat. Die Einrichtung eines Compliance-Management-Systems entfaltet somit eine Art „Strafmilderungswirkung". Ähnlich ist die Wirkung beim FCPA. Obwohl dieses Gesetz keine expliziten Anforderungen an ein Compliance-Programm stellt, wird das Vorliegen eines Compliance-Management-Systems als Strafzumessungsprivileg berücksichtigt.[26]

Das US-Justizministerium sowie die US-Börsenaufsicht veröffentlichen regelmäßig Leitfäden, in welchen die Effektivität eines Compliance-Management-Systems beurteilt wird. Schwerpunktmäßig wird dabei auf das Aufdecken von Fehlverhalten im Unternehmen und die Verhinderung derartiger Verhaltensweisen in Zukunft abgestellt. Die Richtlinie des US-Justizministeriums gibt dabei die Erwartungen und Standards wieder, welche US-Staatsanwälte bei der Bewertung von Compliance-Programmen während einer Untersuchung anwenden.[27]

---

[24] *Kalss* in *Kalss/ Torggler*, Beiträge zum 4. Unternehmensrechtstag (2016) 2
[25] *Erwin-Fierel-Giedenbacher/Karin Mair* in *Peter Lewisch*, Zauberwort Compliance? 17
[26] *Petsche/Larcher* in *Petsche/Mair*, Handbuch Compliance³, 25ff
[27] Vgl. dazu *Schwab*: "DOJ erneuert seine Leitlinien zur Evaluierung von Compliance-Programmen und den FCPA-Leitfaden", Compliance Praxis 3/2020, 40-41

F. Compliance beziehungsweise Compliance-Management-Systeme unabhängig von Unternehmensgröße und -aktivität?

Zum einen ergeben sich aus einschlägigen gesetzlichen Bestimmungen gewisse materiellrechtliche Compliance-Verpflichtungen – so wird beispielsweise ein Immobilienmakler nicht umhinkommen, bei Durchführung gewisser, risikobehafteter Transaktionen, die entsprechenden Bestimmungen zur Verhinderung von Geldwäsche und Terrorismusfinanzierung zu beachten.

Relevant ist auch der Umstand, ob ein Unternehmen an der Börse notiert ist. Ist dies der Fall, gelten einschlägige Kapitalmarkt-Compliance-relevante Regelungen.

Zum anderen ergibt sich aus einer durchgeführten Risiko-Analyse, welche Risiken in welchem Ausmaß bei einem Unternehmen bestehen, wie diese sich realisieren können und wo es sinnvoll erscheint, Gegenmaßnahmen zu implementieren.

Bei Compliance geht es vor allem aber auch um eine Kosten-Nutzen-Analyse. Der im Interesse der Vermeidung von Haftungs- und Strafbarkeitsrisiken für ein Unternehmen getätigte Präventionsaufwand sei keine konstante Größe, sondern beurteile sich abhängig von den jeweiligen Kosten und Nutzen. So formuliert *Kalss* zutreffend, dass die zu erwartenden Nutzen rechtswidrigen Verhaltens gestiegen sein mögen. Die Kosten rechtswidrigen Verhaltens (und das Nutzen ihrer Prävention) seien aber noch mehr gestiegen. So habe sich nicht nur das Portfolio an möglichen rechtlichen Folgen gegen ein Unternehmen erweitert, sondern auch die Häufigkeit entsprechender Sanktionierungen. Jene schließt daraus, der Anstieg in den Kosten rechtswidrigen Verhaltens führe umgekehrt zu einem erhöhten Nutzen entsprechenden „Verhinderungsaufwands“.[28]

Dies wiederum bedeutet im Umkehrschluss, dass kleinere Unternehmen, welche weniger risikobehaftete Aktivitäten als Unternehmensgegenstand haben und nur im Inland oder in weniger stark regulierten Märkten tätig sind, nach der zuvor erwähnten durchzuführenden Risiko-Analyse als auch der Kosten-Nutzen-Analyse oftmals zum Schluss kommen werden, es bedürfe keiner oder nur auf einen gewissen Bereich eingeschränkten Compliance-Aktivitäten.

[28] *Kalss* in *Kalss/ Torggler*, Beiträge zum 4. Unternehmensrechtstag (2016) 2

II. Compliance-Risiken in der Immobilienbranche

Die Immobilienwirtschaft unterliegt per se keinen strengen Regulatorien. Dementsprechend ist die Implementierung und Befolgung von Compliance-Anforderungen für viele Unternehmen in der Branche noch keine Selbstverständlichkeit.

Dies darf weder zum Schluss führen, dass es in der Branche nicht bereits zunehmend zu einem Umdenken kommt, noch, in der Immobilienwirtschaft bestünden keine Compliance Risiken.

In der Immobilienwirtschaft sind primär folgende Themenbereiche - Compliance Risikofelder - relevant:

- Korruption

- Kartellrecht

- Geldwäsche

- Datenschutz

- Exportkontrollbestimmungen (inkl. Finanzsanktionen)

Für die unternehmensspezifische Compliance-Risikoanalyse werden des Weiteren oftmals folgende Bereiche einbezogen: Umwelt- und Menschenrechte, Kapitalmarktrecht, Recht auf geistiges Eigentum (IP-Recht), Produkthaftungsrecht, Arbeitsschutzbestimmungen, Interessenkonflikte (kann auch als Teil des Korruptions-Risikos dargestellt werden).

III. Bestehende Compliance-Regelungen im materiellen Recht

A. Geldwäsche

Geldwäschebestimmungen für Immobilienmakler, Rechtsanwälte und Notare

In Österreich bestehen einschlägige gesetzliche Bestimmungen, welche auf bestimmte Materien beschränkte Pflichten zur Einrichtung organisatorischer Legalitätskontrollfunktionen einführen. Hier primär relevant sind die Geldwäschepräventionsbestimmungen in § 365m ff GewO[29], welche gewisse organisatorische Verpflichtungen vorsehen und sohin als Compliance Maßnahmen im weiteren Sinn zu sehen sind.

Im folgenden Kapitel werden vorrangig die einschlägigen Bestimmungen betreffend Immobilienmakler dargestellt. Des Weiteren werden kurz die anwendbaren Regelungen und Besonderheiten für Rechtsanwälte und Notare dargelegt.

1. Immobilienmakler:

Die relevanten Bestimmungen ergeben sich aus §§ 365m bis 365z GewO (Maßnahmen zur Verhinderung der Geldwäsche und der Terrorismusfinanzierung). Die Regelungen dienen zur Umsetzung der Geldwäscherichtlinie der EU, welche die Verhinderung der Nutzung des Finanzsystems der EU zum Zwecke der Geldwäsche und Terrorismusfinanzierung vorsieht.

Wie sich aus den erläuternden Bemerkungen ergibt, besteht gerade bei Immobiliengeschäften durch den möglichen Wertanlagecharakter solcher Geschäfte ein potenzielles Geldwäscherisiko[30].

Das Gesetz sieht – unter anderem - für Immobilienmakler gewisse Verpflichtungen vor (§ 365m Abs. 2 Z 2 GewO). Diese Bestimmungen gelten gemäß § 365 m1 Z 2 GewO insbesondere im Hinblick sowohl auf Käufer als auch auf Verkäufer beziehungsweise sowohl auf Mieter als auch Vermieter, aber nur in Bezug auf Transaktionen, bei denen sich die monatliche Miete auf EUR 10.000 oder mehr beläuft.

Als konkrete Maßnahmen, welche Gelwäsche und Terrorismusfinanzierung vermeiden sollen, hat der Immobilienmakler gemäß §365n1 GewO „*angemessene Schritte zu unternehmen, um die für ihn bestehenden Risiken der Geldwäsche und Terrorismusfinanzierung unter Berücksichtigung von Risikofaktoren, einschließlich in*

[29] *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II6 § 82 (Stand 1.10.2018, rdb.at) Rz 44
[30] *Gruber/Paliege-Barfuß,* GewO[7] § 365m1 Rz 7 (Stand 1.9.2020, rdb.at)

Bezug auf seine Kunden, Länder oder geografische Gebiete, Produkte, Dienstleistungen, Transaktionen oder Vertriebskanäle zu ermitteln und zu bewerten. Diese Schritte haben in einem angemessenen Verhältnis zu Art und Größe des Unternehmens zu stehen." Der Immobilienmakler ist demnach verpflichtet, eine angemessene Risikobewertung durchzuführen. Dies hat zu erfolgen unter Berücksichtigung unter anderem der Art seiner Kunden (beispielsweise politisch exponierte Personen), der produktbezogenen Risiken, der standortbezogenen Risiken und der Art der Vertriebskanäle.

Absatz 3 des § 365n1 GewO spricht über Strategien, Kontrollen und Verfahren, über welche ein Immobilienmakler zur wirksamen Minderung und Steuerung der ermittelten Risiken zu verfügen hat.

Im Gesetz selbst ist dann in §365n1 Absatz 4 GewO ausgeführt, was darunter zu verstehen ist: die Ausarbeitung interner Grundsätze, Kontrollen und Verfahren, unter anderem in Bezug auf eine vorbildliche Risikomanagementpraxis, Sorgfaltspflichten gegenüber Kunden inklusive Maßnahmen in Bezug auf neue Produkte, Praktiken und Technologien, Verdachtsmeldungen, Aufbewahrung von Unterlagen, interne Kontrolle, Einhaltung der einschlägigen Vorschriften einschließlich der Benennung eines für die Einhaltung der einschlägigen Vorschriften zuständigen Beauftragten auf Führungsebene, wenn dies angesichts des Umfangs und der Art der Geschäftstätigkeit angemessen ist.

Wie von *Gruber/Paliege-Barfuß* ausgeführt, ist demnach wesentlich die Pflicht des Gewerbetreibenden, eine „angemessene" Risikobewertung vorzunehmen, nachvollziehbar aufzuzeichnen, auf aktuellem Stand evident zu halten und der Behörde auf Anfrage in einem allgemein gebräuchlichen Format zur Verfügung zu stellen. Es sind aber auch Strategien, Kontrollen und Verfahren zur wirksamen Minderung und Steuerung der Risiken von Geldwäsche und Terrorismusfinanzierung zu entwickeln und durch den zuständigen Beauftragten auf Leitungsebene zu überwachen[31].

Gemäß den einschlägigen gewerberechtlichen Bestimmungen bestehen allgemeine Sorgfaltspflichten (§ 365o GewO) sowie Sorgfaltspflichten gegenüber Kunden (§ 365p GewO; z.B. Feststellung und Überprüfung der Kundenidentität, Feststellung des wirtschaftlichen Eigentümers, Bewertung und Einholung von Informationen über den Zweck und angestrebte Art der Geschäftsbeziehung). Verstärkte Sorgfaltspflichten gelten

[31] *Gruber/Paliege-Barfuß*, GewO[7] § 365n1

gemäß § 365s GewO gegenüber politisch exponierten Personen als Kunden sowie bei Transaktionen, an welchen Drittländer mit hohem Risiko beteiligt sind.

Die in den einschlägigen Bestimmungen der Gewerbeordnung angeführten Maßnahmen stellen typischerweise Compliance-Aktivitäten dar, welche für den Beruf des Immobilienmaklers sowie andere Gewerbetreibende gesetzlich verankert sind.

2. Rechtsanwälte:

Aus § 8a der Rechtsanwaltsordnung ergibt sich, der Rechtsanwalt ist im Hinblick auf die hohe Gefahr der Geldwäscherei oder Terrorismusfinanzierung verpflichtet, alle Geschäfte, bei denen er im Namen und auf Rechnung seiner Partei Immobilientransaktionen (unter anderem den Kauf oder Verkauf von Immobilien) durchführt oder für seine Partei an deren Planung oder Durchführung mitwirkt, besonders sorgfältig zu prüfen.

Diese Sorgfaltspflicht wird in Absatz 2 der entsprechenden Regelung konkretisiert. Demnach hat der Rechtsanwalt „*angemessene und geeignete Strategien und Verfahren zur Erfüllung der ihm im Rahmen der Bekämpfung von Geldwäscherei (§ 165 StGB) und Terrorismusfinanzierung (§ 278d StGB) auferlegten Sorgfaltspflichten in Ansehung von Parteien, Verdachtsmeldungen, der Aufbewahrung von Aufzeichnungen, interner Kontrolle, Risikobewertung und Risikomanagement sowie zur Sicherstellung der Einhaltung der einschlägigen Vorschriften und der Kommunikation innerhalb seiner Kanzlei einzuführen und aufrechtzuerhalten, um Transaktionen, die mit Geldwäscherei (§ 165 StGB) oder Terrorismusfinanzierung (§ 278d StGB) zusammenhängen, vorzubeugen und diese zu verhindern.“*

Ausdrücklich erfasst sind nach dem Gesetzeswortlaut davon die in einem angemessenen Verhältnis zu seiner konkreten Geschäftstätigkeit und Art und Größe seiner Kanzlei stehenden Strategien, Kontrollen und Verfahren zur wirksamen Minderung und Steuerung der ermittelten Risiken von Geldwäscherei und Terrorismusfinanzierung.

Des Weiteren ergibt sich aus Absatz 2, dass diese Maßnahmen bei Rechtsanwalts-Gesellschaften gegebenenfalls auch die Bestellung eines der Gesellschaft angehörenden Rechtsanwalts zum Compliance-Beauftragten für den Bereich der Verhinderung von Geldwäscherei und Terrorismusfinanzierung umfassen.

Gleichlautend zu den Erfordernissen von Compliance-Management-Systemen ist gemäß dieser standesrechtlichen Regelung festgehalten, die laufende Einhaltung der Strategien, Kontrollen und Verfahren sei zu überwachen, dies gegebenenfalls durch den bestellten

Compliance-Beauftragten. Den Compliance-Grundsätzen entsprechend, ist gesetzlich festgehalten, dass, soweit erforderlich, die getroffenen Maßnahmen zu verbessern sind.

Ausdrücklich geregelt ist darüber hinaus in Absatz 3, der Rechtsanwalt habe „*eine Analyse und Bewertung des für ihn bestehenden Risikos der Inanspruchnahme seiner Tätigkeit zu Zwecken der Terrorismusfinanzierung durchzuführen, wobei dies in einem angemessenen Verhältnis zu seiner konkreten Geschäftstätigkeit und Art und Größe seiner Kanzlei zu stehen hat. Risikofaktoren, die sich bezogen auf seine Kunden, auf bestimmte Länder und geografische Gebiete oder auf bestimmte Produkte, Dienstleistungen, Transaktionen oder Vertriebskanäle ergeben, sind dabei besonders zu berücksichtigen*." Dem Rechtsanwalt wird mit dieser Bestimmung die Verpflichtung auferlegt, eine, den Umständen angemessene, Risikoanalyse vorzunehmen.

Der Oberste Gerichtshof hat dazu konkretisierend festgehalten, die Verpflichtung zur Erstellung einer Risikoanalyse gelte ausnahmslos für jede Anwaltskanzlei. Der, dem verfahrensgegenständlichen Einwand der Entbindung eines Anwalts von der Vornahme einer Risikoanalyse, der der Ansicht war, in seiner Kanzlei lägen keine Risikofaktoren vor, hat der OGH damit eine Absage erteilt.[32]

In Absatz 4 der entsprechenden Regelung wird im Hinblick auf die Verpflichtung des Rechtsanwalts zur Feststellung, ob eine der involvierten Parteien eine politisch exponierte Person ist, ausdrücklich festgehalten, dass der Rechtsanwalt ein in einem angemessenen Verhältnis zu seiner konkreten Geschäftstätigkeit und Art und Größe seiner Kanzlei stehendes, risikobasiertes Verfahren einschließendes Risikomanagementsystem, einzuführen und aufrecht zu erhalten hat. Mit dieser Bestimmung wird dem Prinzip des risikobasierten Ansatzes Rechnung getragen. Es ist dabei die ausdrückliche gesetzliche Verankerung der Einführung eines Verfahrens, inklusive Risikomanagement, hervorzuheben.

3. Notare:

Auch in der Notariatsordnung finden sich Bestimmungen zur Verhinderung der Geldwäsche und Terrorismusfinanzierung, welche Regelungen bezüglich vorzunehmender Risikobewertungen und Risikomanagement enthalten. Die Regelungen sind gleichlautend zu den einschlägigen berufsrechtlichen Bestimmungen in der Rechtsanwaltsordnung.

[32] Dazu OGH vom 22.6.2020, 24 Ds 10/19h

So heißt es im einschlägigen § 36a NO Abs. 1: „*Der Notar ist im Hinblick auf die hier besonders hohe Gefahr der Geldwäscherei (§ 165 StGB) oder Terrorismusfinanzierung (§ 278d StGB) verpflichtet, alle Geschäfte besonders sorgfältig zu prüfen, bei denen er im Namen und auf Rechnung seiner Partei Finanz- oder Immobilientransaktionen (unter anderem den Kauf oder Verkauf von Immobilien oder Unternehmen) durchführt oder für seine Partei an deren Planung oder Durchführung mitwirkt*."

In Absatz 2 ist dazu festgehalten, dass der Notar angemessene und geeignete Strategien und Verfahren zur Erfüllung seiner Sorgfaltspflichten einführen muss, dies unter anderem in Ansehung von Parteien, Verdachtsmeldungen, der Aufbewahrung von Aufzeichnungen, interner Kontrolle, Risikobewertung und Risikomanagement. Zweck der Regelung ist die Vorbeugung und Verhinderung von Transaktionen, die mit Geldwäscherei oder Terrorismusfinanzierung zusammenhängen. Diese Strategien, Kontrollen und Verfahren sind jeweils in einem angemessenen Verhältnis zu seiner konkreten Geschäftstätigkeit und Art und Größe seiner Kanzlei, einzuführen.

Typischerweise für Compliance-Arbeit wird in der einschlägigen Bestimmung festgehalten, dass die laufende Einhaltung der Strategien, Kontrollen und Verfahren zu überwachen ist und allfällige Verbesserungsmaßnahmen zu setzen sind.

Im Hinblick auf Geschäfte mit politisch exponierten Personen treffen Notare die gleichen Verpflichtungen wie Rechtsanwälte. So haben jene ein risikobasiertes Verfahren, einschließlich Risikomanagement, einzuführen und aufrecht zu erhalten.

B. Vergaberecht

§ 26 BVergG – Vermeidung von Interessenkonflikten

Das Bundesvergabegesetz enthält eine klassische Compliance-Regelung. Demnach sind gemäß § 26 BVergG Interessenkonflikte bei Vergabeverfahren zu vermeiden.

Um dies zu bewerkstelligen, gibt der Gesetzgeber Vorgaben, wonach der öffentliche Auftraggeber geeignete Maßnahmen zu treffen hat, um Interessenkonflikte, welche sich bei der Durchführung von Vergabeverfahren ergeben können, wirksam zu verhindern, aufzudecken und zu beheben. Dies mit dem im Gesetz verankerten Ziel, Wettbewerbsverzerrungen zu vermeiden und eine Gleichbehandlung aller Unternehmer zu gewährleisten.

Der Gesetzgeber definiert in Absatz 2 des § 26 BVergG den Begriff des Interessenkonfliktes, wonach ein solcher in jedem Fall dann vorliegt, wenn „*Mitarbeiter eines öffentlichen Auftraggebers oder einer vergebenden Stelle, die an der Durchführung des Vergabeverfahrens beteiligt sind oder Einfluss auf den Ausgang des Verfahrens nehmen können, direkt oder indirekt ein finanzielles, wirtschaftliches oder sonstiges persönliches Interesse haben, das ihre Unparteilichkeit und Unabhängigkeit im Rahmen des Vergabeverfahrens beeinträchtigen könnte."*

Der zentrale Begriff dieser Bestimmung – Interessenkonflikt – wird demnach sehr weit definiert. Der Umfang zeigt sich daran, bei welchem Personenkreis ein solcher Konflikt auftreten kann. Der weite Anwendungsbereich ergibt sich durch die Formulierung „*in jedem Fall (vorliegend)"* am Anfang der Begriffsdefinition. Es ist keine abschließende Definition. Der Begriff wird an objektiven Kriterien festgemacht. Auf subjektive Kriterien stellt die Regelung nicht ab.[33]

Auch der Begriff des „Mitarbeiters" selbst ist weit auszulegen. So ist vom Anwendungsbereich nicht nur das Personal des Auftraggebers oder der vergebenden Stelle umfasst. Auch der Sachverständige fällt darunter. Ebenfalls darunter fallen auch alle Personen, die in einem privat- oder öffentlich-rechtlichen Dienstverhältnis zum Auftraggeber stehen, sowie sonstige Organe und Personen des Verwaltungs-, Leitungs- oder Aufsichtsgremiums des Auftraggebers.[34]

Die Regelung in § 26 BVergG dient als abgeleiteter Grundsatz zu § 20 BVergG, welcher die Gleichbehandlung aller an der Ausschreibung teilnehmenden Unternehmer und einen unverfälschten Wettbewerb gewährleisten soll.[35] So haben *Moik/Gföhler* auf Basis zugrundeliegender EuGH Entscheidungen herausgearbeitet, Ziel der Regelung sei, willkürliche Entscheidungen des öffentlichen Auftraggebers hintanzustellen.[36]

Wie aus den bisherigen Ausführungen zu entnehmen, lässt sich die Regelung vorrangig der Kartellrechtsprävention zuordnen.

Adressat der Bestimmung ist der Auftraggeber. Dieser ist verpflichtet, einerseits im Vorhinein von sich aus und aktiv Vorkehrungen für die Verhinderung von

[33] *Gölles* in *Gölles,* BVergG 2018 § 26 (Stand 1.10.2019, rdb.at) RZ 10f
[34] *Gölles* in *Gölles,* BVergG 2018 § 26 RZ 14 mwN
[35] *Gölles* in *Gölles,* BVergG 2018 § 26 RZ 2
[36] *Moick/Gföhler,* BVergG 2018[1.01] § 26 (Stand 1.3.2021, rdb.at) E1 und E2 mwN

Interessenkonflikten zu treffen, andererseits geeignete Kontrollmaßnahmen für eine Aufdeckung und Behebung eines solchen vorzusehen.[37]

Als geeignete Maßnahmen für Präventiv- und Korrekturmaßnahmen werden in den erläuternden Bemerkungen beispielhaft angeführt:

- Vorbeugende Aufklärungskampagnen des Auftraggebers über Meldepflichten bei Interessenkonflikten

- Einrichtung eines Compliance-Systems

- Einrichtung eines internen Revisions- oder Controlling-Systems

- Anonyme Meldesysteme betreffend Verdachtsfälle

- Personelle Durchgriffsrechte (Suspendierungen, Versetzungen usw.)

Dabei wird auf die einschlägigen Dokumente der OECD und des Europäischen Amtes für Betrugsbekämpfung hingewiesen.[38] Mit den beispielhaft angeführten Maßnahmen, insbesondere der namentlich erwähnten Einrichtung eines Compliance-Systems als potentielle Präventiv- und Korrekturmaßnahme, wird ersichtlich, jene Bestimmung kann (auch) als Grundlage zur Einführung von Compliance-Management-Systemen im Unternehmen herangezogen werden.

Interessant erscheinen in diesem Zusammenhang – neben der eindeutigen Kartellrechtsdimension – weiters die korruptionsrechtlichen Komponenten der Bestimmung. Dies zum einen durch die explizite Erwähnung der einschlägigen korruptionsrechtlichen Materialien relevanter Organisationen, namentlich der OECD sowie des Europäischen Amtes für Betrugsbekämpfung.

Zum anderen wird in der verwandten Bestimmung - Artikel 35 der Richtlinie über die Konzessionsvergabe (RL 2014/23/EU), welche Beschaffungen im Wege von Konzessionsvergaben regelt - die neben den oben dargestellten kartellrechtlichen Erwägungen, nämlich der Vermeidung von Wettbewerbsverzerrungen und der Gleichbehandlung der teilnehmen Unternehmer, auch die Bekämpfung von Betrug, Günstlingswirtschaft und Bestechung angeführt. Bereits die Überschrift zu Artikel 35 zur RL 2014/23/EU – „*Bekämpfung von Bestechung und Verhinderung von*

[37] *Gölles* in *Gölles,* BVergG 2018 § 26 (Stand 1.10.2019, rdb.at) RZ 3f
[38] ErläutRV 69 BlgNR 26. GP 60

Interessenkonflikten“ – lässt keinen Grund, an dem korruptionsrechtlichem Gehalt jener Bestimmung zu zweifeln.

Im April 2021 hat die Europäische Kommission in einer Bekanntmachung zur RL 2014/24/EU die „Leitlinien zur Vermeidung von und zum Umgang mit Interessenkonflikten gemäß der Haushaltsordnung“ veröffentlicht. Der Leitfaden soll helfen, Interessenkonflikte bei der Verwendung von EU-Mitteln – sowohl innerhalb der EU-Institutionen als auch in den Mitgliedstaaten – zu vermeiden. Ausdrücklich angeführt wird die Vermeidung von Günstlingswirtschaft.

Dies soll erreicht werden durch das Anführen konkreter Beispiele. So wird etwa für Vorschriften in Bezug auf Ethik und Interessenkonflikte auf Ebene der Mitgliedstaaten folgendes Beispiel angeführt: *„In einem Mitgliedstaat ist es Parlamentsmitgliedern, Regierungsmitgliedern oder lokalen Führungskräften verboten, eine Person aus dem „engsten Familienkreis“ (Ehepartner, Kinder und Eltern) als parlamentarischen Assistenten oder Mitglied ihres Kabinetts zu beschäftigen. Für die Beschäftigung einer Person aus dem „erweiterten Familienkreis“ (Geschwister, Schwäger, Schwägerinnen, Neffen oder Nichten, frühere Ehepartner etc.) wird in den Rechtsvorschriften die Meldung dieser Beschäftigung vorgesehen.“*

In Abschnitt 5.2 des Leitfadens („*Vorschriften über Interessenkonflikte nach den Vergaberichtlinien*“) ist detailliert dargelegt, welche Vorschriften zur Vermeidung von Interessenkonflikten im Bereich des öffentlichen Auftragswesens bestehen. Nach Artikel 24 der EU-Vergaberichtlinie von 2014 werden Mitgliedstaaten verpflichtet, sicherzustellen, dass die öffentlichen Auftraggeber geeignete Maßnahmen und Systeme einführen, die in der Lage sind, zur wirksamen Verhinderung, Aufdeckung und Behebung von Interessenkonflikten beizutragen, welche sich in allen Phasen des Durchführens von Vergabeverfahren ergeben können.

Unter „Strategien, Vorschriften und Verfahren“ in Abschnitt 6.2 werden die Einführung eines Ethik- und/oder Verhaltenskodex beziehungsweise Regelungen und Verfahren am Arbeitsplatz, einschließlich Vorschriften über den Umgang mit Interessenkonflikten, als hilfreiche Instrumente angeführt, um das Bewusstsein zu schärfen und die Regeln und Pflichten zur Vermeidung und Handhabung von Interessenkonflikten festzulegen.

Der Leitfaden nennt weiters konkrete Themenbereiche, welche in Ethik-/Verhaltenskodices beziehungsweise anderen Instrumenten zur Bewusstseinsschaffung, abgedeckt werden sollten:

- Interessenkonflikte -Erläuterungen, Anforderungen und Meldeverfahren

- Regeln zu Geschenken und Gastfreundschaft

- Regeln zu vertraulichen Informationen

- Anforderungen an die Meldung von Betrugsfällen, einschließlich des Schutzes von Hinweisgebern

Des Weiteren ist detailliert angeführt, dass Rechtsvorschriften, Strategien und förmliche Verfahren zur Regelung von Interessenkonflikten, zur Minderung des Risikos von Interessenkonflikten und zur Bewältigung von Fällen, die auftreten, bereitzustellen sind.

Ein weiterer wichtiger Grundsatz der Compliance-Arbeit, nämlich die laufende Überwachung, Anpassung und allfällige Aktualisierung, wird herausgearbeitet. Gemäß den Ausführungen in dem Leitfaden, müssen in einem ständig verändernden Umfeld die Strategien und Verfahren für den Umgang mit Interessenkonflikten wirksam und relevant bleiben. Dabei sind jene erforderlichenfalls zu aktualisieren.

Ausgeführt wird weiters, die Bediensteten hätten sich zur Einhaltung der festgelegten Vorschriften, Strategien und Verfahren zu verpflichten. Auch dies eine Maßnahme, die sich typischerweise in Compliance-Vorschriften wiederfindet.[39]

C. Versicherungsrecht
   Compliance als „Governance“ und „Internes Kontrollsystem“

Die für Versicherungs- und Rückversicherungsunternehmen geltenden Bestimmungen im Versicherungsaufsichtsgesetz enthalten Compliance-Regelungen, welche im Hinblick auf die Einordnung der Compliance-Funktion sowie deren Aufgabenbereich, über den Versicherungsbereich hinausgehend, relevant sind.

[39] RL 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG des Rates (3) (4) Richtlinie über die öffentliche Auftragsvergabe, 2021/C 121/01

Der 4. Abschnitt im Hauptstück „Governance“ regelt die „Interne Kontrolle, Compliance und interne Revisions-Funktion“. Nach § 108 VAG haben Versicherungs- und Rückversicherungsunternehmen als Governance-Funktionen, neben dem Risikomanagement und der Internen Revision, eine Compliance-Funktion einzurichten.

Gemäß § 117 VAG haben Versicherungs- und Rückversicherungsunternehmen ein wirksames Internes Kontrollsystem einzurichten, welches zumindestens folgende Bereiche umfasst:

(1) Verwaltungs- und Rechnungslegungsverfahren
(2) Interner Kontrollrahmen
(3) Angemessenes Melde- und Berichtswesen auf allen Unternehmensebenen und
(4) Compliance-Funktion

Der Compliance-Funktion und deren Aufgaben werden in § 118 VAG beschrieben. Die dort beispielhaft angeführten Aufgaben umfassen folgende drei Bereiche:

- Beratungsfunktion: Beratung des Vorstands beziehungsweise des Verwaltungsrats und der geschäftsführenden Direktoren in Bezug auf die Einhaltung der für den Betrieb der Vertragsversicherung geltenden Vorschriften

- Überwachungsfunktion: Beurteilung der möglichen Auswirkungen von Änderungen des Rechtsumfelds auf die Tätigkeit des Versicherungs- oder Rückversicherungsunternehmens

- Risiko-Beurteilung: Identifizierung und Beurteilung des mit der Nicht-Einhaltung der rechtlichen Vorgaben verbundenen Risikos (Compliance-Risiko)

Die dort angeführten Compliance-Aufgabenbereiche fassen gut zusammen, was allgemein – auch in jenen Bereichen, wo keine klaren legistischen Regelungen zur Compliance bestehen - zu den Kernaufgaben jener Funktion gezählt werden.

D. Exkurs: Relevante Bestimmungen im Korruptionsstrafrecht

Compliance kommt bei der Vorbeugung strafrechtsrelevanter Handlungen in einem Unternehmen eine wichtige Rolle zu. Dies zum einen um das Unternehmen vor strafrechtlich relevanten Angriffen Dritter oder durch eigene Mitarbeiter zu schützen. Zum anderen um eine strafrechtliche Verantwortlichkeit des Unternehmens und seiner Mitarbeiter zu vermeiden (Organisations- und Überwachungsverschulden).

Im Themenbereich „Criminal Compliance“ stellen die Korruptionsbestimmungen die wichtigsten einschlägigen Rechtsnormen dar. Weitere relevante Delikte im Bereich des Wirtschaftsstrafrechts sind unter anderem Untreue, Betrug, Gläubigerschutzdelikte und Veruntreuung. Im Folgenden soll auf die Kernbestimmungen im österreichischen Strafrecht eingegangen werden. Dies unter besonderer Berücksichtigung der relevanten Aspekte für Bau- und Immobilienunternehmen.

Einschlägige Bestimmungen finden sich zum Großteil im österreichischen Strafgesetzbuch. Hier vor allem relevant sind die Korruptionsbestimmungen im österreichischen Strafrecht (§§ 302ff Strafgesetzbuch, StGB). Die §§ 304 bis 309 StGB, welche sich im 22. Abschnitt des Besonderen Teils des StGB befinden, regeln die Korruptionsstraftatbestände wie Bestechung und Bestechlichkeit, Vorteilszuwendung und Vorteilsannahme. Diese Bestimmungen werden auch als „eigentliche Korruptionsbestimmungen“ bezeichnet.

Ergänzt werden diese eigentlichen Korruptionsbestimmungen durch Amts- und Vermögensdelikte, welche zum Korruptionsrecht im weiteren Sinn gezählt werden, wie etwa Veruntreuung (§ 133 StGB), Untreue (§ 153 StGB) und Geschenkannahme durch Machthaber (§153a StGB).

Zahlreiche andere korruptionsrechtlich relevante Bestimmungen finden sich in Sondergesetzen, wie zum Beispiel dem Lobbying-Gesetz. Oftmals bestehen branchenspezifische Regelungen. Einen wichtigen Bereich stellen die Geldwäschereibestimmungen dar, welche sich vorrangig in branchenspezifischen Regelungen, wie etwa den einschlägigen Bestimmungen im Finanzmarkt-Geldwäschegesetz, im Bankwesengesetz, aber auch in der – für den Immobilien einschlägigen Bereich - Gewerbeordnung, Rechtsanwaltsordnung sowie der Notariatsordnung, finden.

Die Korruptionsbestimmungen im öffentlichen Bereich (Amtsdelikte, §§ 304 bis 308 StGB) schützen ein Allgemeinrechtsgut, das mit der Erfüllung öffentlicher Aufgaben im Zusammenhang steht. Zur genauen Definition dieses Rechtsguts beziehungsweise dem Umfang desjenigen, gibt es unterschiedliche Rechtsmeinungen. Wie sich dem Wiener Kommentar entnehmen lässt, sieht die überwiegende Auffassung die „Sauberkeit, Reinheit und Unverkäuflichkeit der Amtsführung" als geschütztes Rechtsgut an. Bei dem Korruptionsstraftatbestand nach § 309 StGB soll Korruption im privaten Bereich verhindert werden. Zu dieser Bestimmung wird in den erläuternden Bemerkungen der freie lautere Wettbewerb als geschütztes Rechtsgut angeführt.

Wie von *Krakow/Larcher/Petsche/Zareie* richtigerweise dargelegt, ist ein wichtiger Baustein zur Bekämpfung von Korruption die Einführung des Unternehmensstrafrechts, wonach Unternehmen angehalten sind, Überwachungs- und Kontrollmaßnahmen, sohin Compliance-Maßnahmen, zu implementieren, um eine strafrechtliche Verantwortung des Unternehmens hintanzuhalten.

Die Korruptionsbestimmungen im StGB - genauer die Korruptionstatbestände für den öffentlichen Bereich, sohin Bestechlichkeit und Bestechung, Vorteilsannahme und Vorteilszuwendung - nennen als Tatobjekt den Amtsträger (beziehungsweise den Schiedsrichter).

Andere Korruptionsbestimmungen, hier vor allem die Bestimmung zu § 302 StGB, „Missbrauch der Amtsgewalt", sanktionieren bestimmte Verhaltensweisen von Beamten. Alle drei Begriffe – „Amtsträger", „Schiedsrichter" und „Beamter" - sind in § 74 StGB legal definiert. Der Beamtenbegriff ist enger als der Amtsträgerbegriff.

Der Amtsträgerbegriff umfasst drei Alternativen. So wird entweder auf die organisatorische Zugehörigkeit im Sinne einer organisatorischen Einbindung (als Organ oder Dienstnehmer) in einer der im Gesetz angeführten Körperschaften, wie etwa dem Bund, Land oder der Gemeinde, oder einer anderen Person des öffentlichen Rechts (lit. b) oder auf die funktionelle Ausübung der Tätigkeiten, sohin der Vornahme von Amtsgeschäften, (lit. c) abgestellt (funktionaler Amtsträgerbegriff).

Die dritte Alternative (lit. d) stellt auf die Amtsträgereigenschaft durch Beteiligung sowie durch Beherrschung (durch die im Gesetz angeführten Gebietskörperschaften) beziehungsweise auf die Amtsträgereigenschaft durch die Rechnungshofkontrolle ab.

So fallen unter den Begriff des Amtsträgers Organe oder Bedienstete eines Unternehmens, an dem eine Gebietskörperschaft (beziehungsweise mehrere Gebietskörperschaften zusammen) zu 50% oder mehr beteiligt ist oder welches auf sonstige Weise von einer Gebietskörperschaft beherrscht wird.

Neben der Beteiligung und Beherrschung eines Unternehmens durch eine beziehungsweise mehrere Gebietskörperschaften fallen auch all jene Organe beziehungsweise Bedienstete eines Unternehmens, dessen Gebarung der Überprüfung durch den Rechnungshof unterliegt, unter den Amtsträgerbegriff.

Der Amtsträgerbegriff ist sohin sehr weit zu interpretieren. Insbesondere durch die in lit. d eingeführte Variante fallen unter den Amtsträgerbegriff auch Organe und Bedienstete von Unternehmen, wie etwa der ASFINAG, der Wiener Linien, der ÖBB, des ORF und Universitäten. Als Beispiel im Immobilienbereich zu nennen sind die Organe und Bedienstete der Bundesimmobiliengesellschaft (BIG), welche als Amtsträger einzustufen und sohin in den Anwendungsbereich der eigentlichen Korruptionsdelikte fallen.

Zusätzlich zu Korruptionsdelikten im öffentlichen Sektor, werden Korruptionshandlungen im privaten Bereich nach § 309 StGB (Geschenkannahme und Bestechung von Bediensteten und Beauftragten) geahndet, und zwar die aktive Bestechung und die passive Bestechlichkeit.

Für international tätige Unternehmen sind weiters der UK Bribery Act sowie der US FCPA relevante gesetzliche Bestimmungen, welche sich von der Gesetzessystematik, insbesondere aber auch vom Anwendungsbereich, deutlich unterscheiden zu den österreichischen Gesetzesbestimmungen.

E. Exkurs: Kartellrecht

Kartellrechtliche Verstöße stellen im Immobilienbereich einen praktisch äußerst relevanten Bereich dar, wie man auch an den medial kolportierten Fällen sehen kann. Neben dieser materiellrechtlichen Komponente haben Übertretungen der Kartellrechtsregelungen wesentlich zur Entwicklung von Compliance-Management-Systemen und Regelwerken beigetragen. Des Weiteren sind es die Kartellbehörden und -gerichte, welche Compliance-Management-Systeme regelmäßig als Strafmilderungsgründe bei der Strafbemessung einstufen und deren Wirkung und Sinnhaftigkeit somit indirekt bestätigen und weiterentwickeln. Es sollen hier folgende Urteile des Kartellgerichts beispielhaft angeführt werden:

In dem im Oktober 2021 ergangenen Urteil des Kartellgerichts zu dem Baukartell (Preisabsprachen, Marktaufteilung, Informationsaustausch) rund um namhafte österreichische Baukonzerne – namentlich der STRABAG AG zu 27 Kt 12/21y – hat das Kartellgericht klar festgehalten, dass sich die Einführung eines zertifizierten Compliance-Systems in Verbindung mit einem neuartigen Monitoring-System mildernd auf das Strafausmaß ausgewirkt hat. So hat das darin involvierte Immobilienunternehmen STRABAG AG, welches sich zur Einführung und der Umsetzung der Compliance-Maßnahmen verpflichtet hat, eine deutlich mildere Strafe ausgefasst als andere ebenfalls involvierte Unternehmen.

Auch im Urteil 25 Kt 76/14, in welchem das Kartellgericht gegen Vöslauer Mineralwasser AG vertikale Preisabstimmungen bei nichtalkoholischen Getränken im Lebensmitteleinzelhandel festgestellt und eine Strafe verhängt hat, hat die freiwillige endgültige Beendigung der kartellrechtswidrigen Verhaltensweisen und damit im Zusammenhang stehend die Einführung eines Compliance-Programms – zu einem 20%igen Nachlass bei der Strafbemessung geführt.

Im Fall zu 26 Kt 105/13, in welchem vertikale Preisabstimmungen im Lebensmitteleinzelhandel (Molkereiprodukte von Emmi Österreich GmbH) den Verhandlungsgegenstand bildeten und bei den involvierten Unternehmen festgestellt worden sind, hat das Kartellgericht in seiner Begründung angeführt, die Compliance-Anstrengungen der Antragsgegnerin nach der Hausdurchsuchung, zusammen mit der Kooperation bei der Aufklärung, haben zu einem 10%igen Nachlass bei der Strafbemessung geführt.

IV. Rechtliche Verpflichtung zur Implementierung eines Compliance-Management-Systems?

Eine Verpflichtung zur Compliance Organisation wird vom österreichischen Gesetzgeber mit Ausnahme einzelner einschlägiger Bestimmungen (hier vor allem wertpapierrechtliche Regelungen, Regelungen im Bankwesengesetz und Versicherungsaufsichtsgesetz), nicht explizit vorgeschrieben.

Dies gilt umso mehr für den Immobiliensektor. Hier bestehen lediglich einzelne (Compliance-)Regelungen im Hinblick auf spezifische Materien, wie etwa die Bestimmungen zur Geldwäschebekämpfung für definierte Berufsgruppen.

In diesem Kapitel möchte ich auf die Frage eingehen, ob es eine – indirekte – Verpflichtung zur Einführung eines Compliance-Management-Systems gibt. Dazu werden in den Unterkapiteln die jeweiligen einschlägigen Bestimmungen dargestellt sowie weiters auf den Begriff und das Instrument der – für die Compliance-Arbeit immanenten – Risikoanalyse eingegangen.

A. Gesellschaftsrecht (Aktiengesetz und GmbH-Gesetz)

1. Pflicht zur Einführung eines internen Kontrollsystems

In den österreichischen Gesetzen finden sich Bestimmungen, wonach die Einführung eines internen Kontrollsystems Aufgabe des Vorstands (§ 82 AktG) beziehungsweise des Geschäftsführers (§ 22 Abs. 1 GmbHG) ist. Ein internes Kontrollsystem wird dabei als die Gesamtheit aller prozessbezogenen Überwachungsmaßnahmen einer Organisation verstanden.[40]

Hinsichtlich der aktienrechtlichen Bestimmungen wird gemäß *Reich-Rohrwig/Zimmermann* in *Artmann/Karollus*, Kommentar zum AktG, das interne Kontrollsystem wie folgt definiert: „*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*“.[14]

Im Zusammenhang mit den Pflichten zur Führung eines internen Kontrollsystems eröffnet sich die Diskussion, ob der Vorstand auch zur Einrichtung eines umfassenden Risikomanagementsystems beziehungsweise einer Compliance-Organisation verpflichtet

[40] *Petsche/Mair*, Handbuch Compliance³ 29

ist.[41] Gemäß *Reich-Rohrwig/Zimmermann* wird dies als weitergehende, aus der Legalitätspflicht des Vorstands entspringende, organisatorische Pflicht diskutiert.[42] Unter der Legalitätspflicht wird dabei die Pflicht des Vorstands selbst zum rechtmäßigen Handeln verstanden.

Bei der Frage nach dem Erfordernis der Einrichtung eines Compliance-Management-Systems geht es hingegen um die Frage, ob und inwieweit den Vorstand die Pflicht trifft, durch Kontrollsysteme dafür Sorge zu tragen, dass auch Dritte, insbesondere Mitarbeiter, Handelsvertreter, Subunternehmer, ihrer Legalitätspflicht bei ihrer Tätigkeit für die Gesellschaft umfassend nachkommen. Es wird hier in der Literatur auch von der „Legalitätskontrollpflicht" gesprochen. In diesem Zusammenhang von Interesse ist wohl auch, inwieweit die Business Judgement Rule bei der Ausgestaltung eines solchen Compliance-Management-Systems eine Rolle spielt.

In Deutschland besteht dazu die herrschende und in Österreich die verbreitete Meinung, welche eine Verpflichtung zur Legalitätskontrolle und sohin das „ob" der Einrichtung einer Compliance-Organisation befürwortet. Zugleich wird dem Vorstand ein weiter Ermessenspielraum bei der Ausgestaltung eines solchen Systems, also beim „Wie" der Implementierung einer Compliance-Organisation, zugestanden.[43] Dieser Ermessensspielraum der Verantwortlichen bei der Ausgestaltung des Compliance-Management-Systems richtet sich nach der Unternehmensgröße und der Risikoexponiertheit beziehungsweise der Gefahrenlage, in welchem das Unternehmen tätig ist.[44]

Wie sich aus der Literatur ergibt, ist die Diskussion um den Ermessensspielraum maßgeblich vom „Siemens/Neubürger"-Urteil geprägt, in welchem das LG München I als erstinstanzliches Gericht aussprach, dass der Vorstand seine Organisationspflicht nur dann erfülle, wenn er bei entsprechender Gefährdungslage eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation einrichtet. Umgekehrt verletze der Vorstand seine Legalitätspflicht, wenn er es unterlässt, die Effizienz dieses Systems sicherzustellen.[45] Des Weiteren kann dem „Siemens/Neubürger" Urteil entnommen werden, dass es bei gehäuften Rechtsverletzungen, welche „tiefergreifende,

[41]. *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II[6] § 82 Rz 7
[42] *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II[6] § 82 Rz 34
[43] *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II[6] § 82 Rz 35f
[44] *Kalss* in *Kalss/ Torggler*, Beiträge zum 4. Unternehmensrechtstag (2016) 11
[45] *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II[6] § 82 Rz 36 mwN

organisatorische Unzulänglichkeiten“ vermuten lassen, die Pflicht ergeben kann, Überwachungssysteme im Sinne eines umfassenden Compliance-Management-Systems zu etablieren.[46]

Im „Siemens/Neubürger“ Urteil ist der Vorstand in dem zugrundeliegenden Fall wegen mangelnder Korruptionsprävention zum Ersatz der dadurch entstandenen Schäden verurteilt worden, ohne dass das Gericht auf die Ermessensfrage einging. Dies wird in der Literatur damit argumentiert, dass sich der Ermessenspielraum dann für den Vorstand verengt, wenn es im Unternehmen bereits zu einschlägigen Rechtsverstößen gekommen ist.[47] Im Umkehrschluss bedeutet dies, das Fehlen eines qualifizierten Verdachts oder die Kenntnis gehäufter Rechtsverletzungen führen zu einem Ermessen des Vorstands im Hinblick auf die Einführung eines Compliance-Management-Systems.

Durchaus kritisch *Reich-Rohrwig/Zimmermann*, welche die Einstufung von Compliance als allgemeine Leitungsaufgabe problematisch sehen, mit der Begründung, dieses Argument würde für alle anderen Leitungsaufgaben (Finanzierung, Informationssystem, Außenkommunikation, Personalwesen etc.) ebenso gelten. Ihres Erachtens führe dies zu einer Verrechtlichung ordnungsgemäßer Unternehmensleitung unter Verdrängung von Ermessensspielräumen.[48]

Zusammenfassend ist die Bestimmung bezüglich des internen Kontrollsystems meines Erachtens so zu interpretieren, dass die Einrichtung einer Compliance-Organisation als eine Leitungsaufgabe zu sehen ist, die der Vorstand sorgfältig und vom Unternehmenswohl getragen, aber in seinem weiten Ermessen, zu entscheiden hat. Es scheint dabei legitim und anerkannt, dass der Vorstand hierbei insbesondere eine Risikoabschätzung durchführen wird müssen, die solche Handlungen, aus denen dem Unternehmen ein hoher Schaden droht, beispielsweise aus dem Kartell- beziehungsweise Korruptionsrecht, mit höherem Aufwand zu verhindern anstrebt als weniger schadensträchtige.[49]

Erwähnenswert an dieser Stelle erscheint die Tatsache, dass es keine allgemeingültige Definition eines Compliance-Management-Systems gibt. So bestehen, laut *Reich-Rohrwig/Zimmermann*, Überschneidungen zwischen einem ordentlichen internen Kontrollsystem und typischen Bestandteilen von Compliance-Management-Systemen. Die

[46] *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II⁶ § 82 Rz 41 mwN
[47] *Gregor Bachmann*, Vorstandshaftung in Deutschland, Jüngste Entwicklung und Reformfragen, ecolex 2015, 37
[48] *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II⁶ § 82 Rz 42
[49] *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II⁶ § 82 RZ 38

Trennung von Zahlungsanforderung, Genehmigung und Durchführung von Zahlungen – als klassisches Element von einem internen Kontrollsystem – stellen eine Legalitätskontrollfunktion dar, indem es rechtswidrigen oder rechtsgrundlosen Zahlungen vorbeugt.

Daraus schließen die Autoren, Unternehmen, welche ein ordnungsgemäßes internes Kontrollsystem eingerichtet hätten, würden jedenfalls auch eine „Compliance-Funktion" aufweisen. Diesem Gedanken folgend, hätte die Frage, ob ein Compliance-System einzurichten sei, nur dann weitergehenden Sinn, wenn darunter über das interne Kontrollsystem hinausgehende Elemente verstanden würden. Als Beispiele sind hier zu nennen:

- Compliance-Richtlinien

- Whistleblower-Hotlines

- Compliance-Officer

- Compliance-Audits. [50]

Nähere Ausführungen zur Unterscheidung zwischen Compliance und dem internen Kontrollsystem finden sich im Abschnitt IV.H.

Differenziert äußert sich hierzu *Schopper*. Diesem zufolge lasse sich eine konzernweite Compliance Verantwortung in Bezug auf regelkonformes Verhalten aller nachgeordneten Unternehmen beispielsweise im Hinblick auf die Einhaltung von jedweden kartell-, straf- oder umweltrechtlichen Vorschriften aus §§ 82 AktG und 22 GmbH, welche nur auf die Rechnungslegung Bezug nehmen, nicht ableiten.

Eine allgemeine konzernweite Compliance-Verantwortung für die Geschäftsleiter einer Konzernobergesellschaft lässt sich, seines Erachtens, auch nicht aus anderen Sonderregelungen des AktienG beziehungsweise des GmbHG ableiten, sondern handle es sich, jenem zufolge, um eine Facette der allgemeinen Sorgfalts- und Treuepflicht nach § 25 GmbHG und § 84 AktG. [51]

2. Allgemeine Sorgfalts- und Treuepflichten

Neben den konkreten Pflichten zur Einführung eines internen Kontrollsystems, bestehen die allgemeinen Sorgfalts- und Treuepflichten, welche den Geschäftsführer einer

[50] *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II[6] § 82 Rz 37
[51] *Schopper* in *Kalss* in *Kalss/ Torggler*, Beiträge zum 4. Unternehmensrechtstag (2016) 60

Gesellschaft als auch die Mitglieder des Geschäftsleitungsorgans einer Aktiengesellschaft treffen (§ 25 GmbHG, § 84 AktG). Diese Bestimmungen legen fest, die jeweils führenden Organe einer Gesellschaft haben die Sorgfalt eines ordentlichen Geschäftsmanns anzuwenden. Des Weiteren wird festgehalten, welche Pflichten der Geschäftsführer der Gesellschaft ha. Hierbei handelt es sich um die, die GmbH treffenden öffentlich-rechtlichen Verpflichtungen, wie etwa steuerliche Pflichten.

Aus § 25 GmbHG kann abgeleitet werden, dass die Geschäftsführer auch sonstige öffentlich-rechtliche Pflichten der GmbH zu erfüllen haben, welche das Gesetz der juristischen Person beziehungsweise deren gesetzlichen Vertreter auferlegt hat. Gemäß *Reich-Rohrwig* gehören dazu, neben der Einhaltung gewerbe- und betriebsanlagenrechtlicher sowie arbeits-, arbeitsverfassungs- und arbeitnehmerschutzrechtlicher Vorschriften auch kartellrechtliche Regeln und Bestimmungen.

Weiters führt jener aus, dass, für den Fall, wenn die GmbH durch öffentliches Angebot Wertpapiere ausgibt, z.B. Anleihen, den Geschäftsführer die Verpflichtung zur Einhaltung der Vorschriften des Kapitalmarktgesetzes, bei Börsennotierung auch die dafür relevanten börserechtlichen Bestimmungen, wie etwas dem Verbot des Insiderhandels als auch der Emittenten-Compliance (die dafür einschlägige ECV – Emittenten-Compliance-Verordnung, ist mittlerweile aufgehoben worden).

Wie des Weiteren von *Reich-Rohrwig* ins Treffen geführt, treffen den Geschäftsführer auch Überwachungs- und Sorgfaltspflichten, dies im Zusammenhang mit Geldwäscherei und Terrorismusfinanzierung. Wie bereits im einschlägigen Kapitel „Geldwäsche“ aufgezeigt, hat bei geldwäschegeneigten Geschäften (z.B. Bareinzahlungen, Kauf von Immobilien) gegebenenfalls eine Feststellung des wirtschaftlichen Eigentümers zu erfolgen. [52]

Die oben angeführten, vom Geschäftsführer der Gesellschaft als gesetzlicher Vertreter der GmbH, einzuhaltenden Maßnahmen sind jene, welche weitegehend als „Compliance-Maßnahmen“ definiert und bekannt sind.

Einzelne Stimmen in der Literatur, so unter anderem *Bernhard Kofler-Senoner,* leiten aus den Bestimmungen über die, den Geschäftsführer/die Geschäftsleitung treffenden, allgemeinen Sorgfalts- und Treuepflichten, explizit eine unmittelbare Verpflichtung zur Implementierung effizienter Compliance-Maßnahmen ab. Demzufolge sind

[52] *Reich-Rohrwig* in *Straube/Ratka/Rauter*, WK GmbHG § 25 (Stand 1.6.2015, rdb.at), Rz 18

Vorstandsmitglieder/Geschäftsführer, die ihre Obliegenheiten verletzen, der Gesellschaft gegenüber zum Ersatz des daraus entstandenen Schadens als Gesamtschuldner verpflichtet. Auch Aufsichtsratsmitglieder haben in ihrem Aufgabenbereich entsprechende Sorgfaltspflichten zu wahren [53]

So argumentiert auch *Jaufer* gemäß der Bestimmung, wonach der Vorstand die Gesellschaft mit der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters unter eigener Verantwortung zu leiten hat, der Vorstand habe eine unternehmensweite Organisationsverantwortung wahrzunehmen und es treffe ihn daher die Verpflichtung, auf ein rechtmäßiges Verhalten auf allen Ebenen des Unternehmens (Legalitätskontrolle) hinzuwirken. Des Weiteren führt dieser, basierend auf den allgemeinen Sorgfalts- und Treuepflichten, aus, es bestünde bei entsprechender Größe, Komplexität und Risikogeneigtheit eines Unternehmens im Rahmen einer sorgfältigen Geschäftsleitung die Pflicht zur Etablierung einer adäquaten - somit einer den Anforderungen des Unternehmens entsprechenden - Compliance Organisation, deren Kernaufgabe die Sicherstellung des rechtmäßigen Verhaltens im Unternehmen zur Minimierung und Vermeidung von Risiken ist. Dementsprechend kommt jener zur Conclusio, dass die Einrichtung eines Compliance-Management-Systems nicht nur empfehlenswert, sondern erforderlich sei.

Interessant erscheint an der Argumentation von *Jaufe*, dass er bei den, diesen Schlussfolgerungen zugrundeliegenden Ausführungen, die Wechselwirkung zwischen Insolvenzprophylaxebestimmungen und Compliance hervorhebt.

Jaufer gelangt dabei zum Schluss, Insolvenzprophylaxebestimmungen seien Rechtsgrundlage für eine funktionierende Corporate Compliance. Des Weiteren argumentiert jener, die Insolvenzprophylaxebestimmungen des Unternehmens- und Gesellschaftsrechts würden wesentliche Elemente einer ordnungsgemäßen Corporate Compliance darstellen. [54]

B. Verwaltungsstrafrecht (VStG)

Im Hinblick auf die Frage nach der Verpflichtung zur Einführung eines Compliance-Management-Systems sind auch die einschlägigen Bestimmungen im Verwaltungsstrafrecht (VStG) relevant, hier vor allem die Bestimmung des § 9 VStG. Gemäß § 9 Absatz 6 VStG wird eine Mithaftung der juristischen Person für die – den

[53] *Kofler-Senoner* in *Peter Lewisch*, Zauberwort Compliance? 63
[54] *Jaufer* in SWK 19/2011, W 41

Unternehmensorganen und verantwortlichen Beauftragten auferlegten – Geldstrafen normiert. Dabei legt § 9 VStG die das Unternehmen betreffenden Pflichten auf die Leitungsorgane um. Es gilt Schuldstrafrecht. Die Leitungsorgane haben, für die im Unternehmen verwirklichten, verwaltungsstrafrechtlichen Verstöße nur aufgrund des eigenen Verschuldens, nämlich des eigenen Organisations- und Überwachungsverschuldens, einzustehen. Die Leitungsorgane haben dementsprechend ein vernünftiges Regel- und Kontrollsystem einzurichten, das Rechtsverstöße verhindert.

Es wird von einigen Literaturmeinungen dementsprechend aus § 9 VStG die Verpflichtung der Leitungsorgane zur Einrichtung eines Kontrollsystems abgeleitet. Aus der Norm beziehungsweise der einschlägigen Rechtsprechung ergeben sich keine konkreten Anforderungen, vielmehr ergibt sich zum Ausmaß die Leitlinie, der Kontroll- und Präventionsaufwand habe in einem angemessenen Verhältnis zu den ansonsten zu befürchtenden Nachteilen (Schäden) zu stehen. Gemäß der Rechtsprechung des VwGH liegt keine Pflichtwidrigkeit der Leitungsorgane vor, wenn die diesbezüglich getroffenen Maßnahmen solche sind, die „*unter den vorhersehbaren Verhältnissen die Einhaltung der gesetzlichen Vorschriften aus gutem Grund erwarten lassen*".[55] So ergibt sich aus dem Erkenntnis des VwGH vom 23.4.1996 (GZ 95/11/0411), dass dem Organ der juristischen Person im Sinne des § 9 Abs. 1 VStG (hier der Arbeitgeber der GmbH im Hinblick auf die Übertretung arbeitsrechtlicher Bestimmungen) die Unterlassung der Einrichtung oder Dartun eines solchen Kontrollsystems nur dann zur Last fällt, wenn sich:

a) tatsächlich Verstöße ereignet haben und

b) diese Verstöße durch das Kontrollsystem hätten verhindert werden können.

Wenn ein an sich taugliches Kontrollsystem in einem Einzelfall versagt hätte, kann sein Fehlen nicht zur Strafbarkeit des Arbeitgebers führen, weil dies im Ergebnis zu einer nach dem Gesetz nicht gegebenen Strafbarkeit führen würde.[56]

Ein früheres Vorstandsmitglied von Siemens wurde 2013 zur Zahlung von 15 Millionen Euro Schadenersatz an Siemens verurteilt. Das Vorstandsmitglied wurde zur Haftung herangezogen, weil es - obwohl nicht speziell ressortzuständig für Compliance - von gravierenden Missständen betreffend vermutete Schmiergeldzahlungen informiert worden war, aber nichts Ausreichendes unternommen hatte, um Abhilfe zu schaffen. Das LG München stellte fest, dass ein Vorstandsmitglied dafür sorgen müsse, das Unternehmen so

[55] *Peter Lewisch* in *Peter Lewisch*, Zauberwort Compliance? S 4
[56] VwGH 23.4.1996, 95/11/0411

zu organisieren und zu beaufsichtigen, dass keine derartigen Gesetzesverletzungen stattfänden. Dieser Organisationspflicht genüge der Vorstand bei entsprechender Gefährdungslage nur dann, wenn er eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation einrichtet. Die Einrichtung eines mangelhaften Compliance-Systems und auch dessen unzureichende Überwachung bedeuteten eine Pflichtverletzung des Vorstandes.[57]

C. Verbandsverantwortlichkeitsgesetz (VbVG)

Wichtigste Bestimmung im Hinblick auf verbandsbezogene Verantwortlichkeit im Strafrecht ist das Verbandsverantwortlichkeitsgesetz, auch als Unternehmensstrafrecht bekannt. Demnach kann, neben der individuellen strafrechtlichen Verantwortlichkeit der handelnden Personen, auch das Unternehmen strafrechtlich nach dem Verbandsverantwortlichkeitsgesetz (VbVG) zur Verantwortung gezogen werden, wenn die im VbVG definierten Kriterien erfüllt sind. Sohin können dem Unternehmen auch strafrechtliche Sanktionen drohen für den Fall, wenn Entscheidungsträger oder Mitarbeiter des Unternehmens eine strafbare Handlung, beispielsweise ein Korruptionsdelikt, setzen und dies dem Unternehmen zugerechnet werden kann.

Zugerechnet werden kann die Tat dem Verband, wenn entweder die Straftat zugunsten des Unternehmens (GmbH, Aktiengesellschaft, etc.) begangen worden ist oder durch die Straftat Pflichten verletzt wurden, die den Verband treffen. Für Straftaten kann der Verband grundsätzlich dann belangt werden, wenn die Entscheidungsträger (Geschäftsführer, Vorstandsebene etc.) die nach den Umständen gebotene und zumutbare Sorgfalt außer Acht gelassen haben. Insbesondere, wenn sie wesentliche technische, organisatorische und personelle Maßnahmen zur Verhinderung solcher Taten unterlassen haben.

Wie von *Helmut Fuchs* herausgearbeitet, geht es dem Gesetz gerade um die Schaffung eines Umfeldes, das die Gefahr der Begehung von Straftaten vermindert – und genau das streben auch die Compliance-Regeln an.[58]

Die Bedeutung von Compliance-Management-Systemen ist im Hinblick auf das Verbandsverantwortlichkeitsgesetz vornehmlich bei der Mitarbeiterstraftat verankert. So ergibt sich aus dem *Wiener Kommentar zum Strafgesetzbuch*, dass dann, wenn die Kriterien der vorsätzlichen beziehungsweise fahrlässigen Mitarbeiter-Anlasstat erfüllt sind, die

[57] *Georg Schima*, Arbeitsrechtliche Grenzen der Compliance, DRdA 2014, 197
[58] *Helmut Fuchs* in in *Peter Lewisch*, Zauberwort Compliance? 33

strafrechtliche Verantwortlichkeit des Verbandes zusätzlich davon abhängt, ob die Tatbegehung dadurch ermöglicht oder zumindest wesentlich erleichtert wurde, dass Entscheidungsträger nicht die gebotene und zumutbare Sorgfalt zur Verhinderung solcher Taten aufgewendet haben.

Weiters ergibt sich aus dem Gesetz, dass Entscheidungsträger insbesondere technische, organisatorische und personelle Maßnahmen zur Tatverhinderung zu setzen haben, soweit sie nach den Umständen geboten und zumutbar sind. Der *Wiener Kommentar zum Strafgesetzbuch* nennt als Beispiele für technische, organisatorische und personelle Maßnahmen namentlich Richtlinien, Schulungen, Wartung, Überwachung, Stichproben und dergleichen. Dabei seien nur mögliche Maßnahmen geboten.[59] Die angeführten Beispiele sind typische Erscheinungsformen der Compliance Arbeit und wesentlicher Bestandteil eines Compliance-Management-Systems.

Des Weiteren ergibt sich aus den genannten einschlägigen Bestimmungen, es ist im Einzelfall zu prüfen, welche Maßnahmen beziehungsweise Vorkehrungen geboten und zumutbar sind. Als entscheidende Faktoren werden dabei unter anderem die Art, Größe, Struktur und Branchenzugehörigkeit des Verbandes angeführt, des Weiteren die Gefährlichkeit des Tätigkeitsbereiches, die Ausbildung und Verlässlichkeit der Mitarbeiter.[60] Die Abstufung nach Risikoexponiertheit des jeweiligen Unternehmens ist typisch für die Compliance-Arbeit.

Nach *Petsche/Larcher* ist die Bestimmung in § 3 Abs. 3 VbVG derartig zu deuten, dass durch das Kontrollversagen ermöglichte Handeln von Mitarbeitern die Verbandsverantwortlichkeit ausgelöst wird und dies im Umkehrschluss bedeutet, dass die Implementierung eines effizienten Compliance-Management-Systems die Strafbarkeit des Unternehmens verhindern kann.[61]

So führt auch *Fuchs* aus, dem Verbandsverantwortlichkeitsgesetz gehe es ja gerade um die Schaffung eines Umfeldes, das die Gefahr der Begehung von Straftaten vermindert. Dies streben genau Compliance-Regeln an. Er kommt sohin zum Schluss, Unternehmen schützen sich durch Compliance-Regeln gegen die Verbandshaftung.[62]

---

[59] *Lehmkuhl/Zeder* in *Höpfel/Ratz,* WK² VbVG § 3 Rz 41
[60] *Lehmkuhl/Zeder* in *Höpfel/Ratz,* WK² VbVG § 3 Rz 42 mwN
[61] *Petsche/Mair*, Handbuch Compliance³ 32
[62] *Helmut Fuchs* in in *Peter Lewisch*, Zauberwort Compliance? 33

Hinsichtlich des Zusammenhanges zwischen Sorgfaltspflichtverletzung auf Entscheidungsträgerebene und Mitarbeiter-Anlasstat wird vom Gesetz nicht auf ein strenges Kausalitätserfordernis abgestellt. Vielmehr wird die Risikoerhöhung für ausreichend erachtet. Die gebotenen und zumutbaren Maßnahmen hätten die Tat nicht mit an Sicherheit grenzender Wahrscheinlichkeit verhindern können, doch ihre Begehung wesentlich erschwert.[63]

Wie von *Petsche/Larcher* herausgearbeitet, wird es bereits im eigenen Interesse der jeweiligen Geschäftsleitung (Vermeidung einer persönlichen Haftung) sein, eine Compliance-Organisation aufzubauen. Dadurch können vor allem rechtliche Fehlerquellen minimiert werden und die Geschäftsleitung kann sich gegenüber der Gesellschaft und/oder Dritten absichern. Gleichzeitig, so kommen *Petsche/Larcher* zum Schluss, wird das Risiko der Bestrafung des Unternehmens selbst reduziert.[64]

D. Corporate Governance Kodex

Der Begriff „Corporate Governance" ist im Verhältnis zum Begriff „Compliance" weiter, weil er alle Regelungen und anerkannten Standards sorgfältiger Unternehmensführung umfasst. Compliance kann dabei als Teil oder wesentlicher Standard einer guten Corporate Governance gesehen werden. Gemäß *Napokoj* beeinhalte eine gute Unternehmensführung wohl eine dem Unternehmen angepasste Compliance-Organisation.

Jener zufolge liegt der Unterschied zwischen Corporate Governance und Compliance in der Perspektive. Während Corporate Governance die Sichtweise der Regulierer prägt, umschreibt Compliance den Blickwinkel der Regulierten, sohin der betroffenen Unternehmen.[65]

Der österreichische Corporate Governance Kodex (ÖCGK) ist ein Ordnungsrahmen für eine verantwortliche, auf nachhaltige und langfristige Wertschaffung ausgerichtete Leitung und Kontrolle von Unternehmen. Der ÖCG enthält drei verschiedene Arten von Regeln als „Best practice" Empfehlungen[66]:

- L Regeln (legal requirements)
- C Regeln (comply or explain) und

[63] *Lehmkuhl/Zeder* in *Höpfel/Ratz,* WK² VbVG § 3 Rz 45 mwN
[64] *Petsche/Larcher* in *Petsche/Mair*, Handbuch Compliance³ 32
[65] *E. Napokoj* in *Napokoj*, Risikominimierung Rz 3
[66] Arbeitsunterlage Corporate Compliance Officer Lehrgang, "Governance & Compliance"

- R Regeln (Recommendations)

Wie von *Petsche/Larcher* aufgezeigt, kann die Verpflichtung zur unternehmensrechtlichen Normierung des ÖCGK im UGB indirekt auch ein Compliance-Programm erfordern.

Interessant erscheinen dabei die folgenden Regelungen:

Punkt 37 ÖCGK, welcher unter anderem vorsieht, der Aufsichtsratsvorsitzende halte mit dem Vorstandsvorsitzenden regelmäßig Kontakt und diskutiert mit ihm über Strategie, die Geschäftsentwicklung und das Risikomanagement des Unternehmens.[67]

Ebenfalls von Relevanz ist die verpflichtende Regelung Nr. 15 des ÖCGK, wonach der Vorstand geeignete Vorkehrungen zur Sicherstellung der Einhaltung der für das Unternehmen relevanten Gesetze zu treffen hat. Diese Bestimmung kann als unbedingte Legalitätskontrollpflicht gedeutet werden.

Gemäß *Schopper* ist die L-Regeln Nr. 15 als eine auf Ebene des Kodex vorgenommene Konkretisierung der allgemeinen Sorgfaltspflicht gemäß § 84 Abs. 1 AktG zu verstehen. Dies bedeute allerdings keine strikte Rechtspflicht. *Schopper* argumentiert hier im Einklang mit der überwiegenden Lehre in Österreich, wonach die Compliance Verantwortung des Vorstands auf Ebene der Einzelgesellschaft zumindestens dem Grunde nach unstrittig ist, als Ausprägung der allgemeinen Sorgfaltsplicht angesehen wird und als unternehmerische Ermessensentscheidung der Business Judgement Rule unterliegt.

Des Weiteren relevant sind die C-Regeln 18a und 70.

Gemäß der „*Comply or explain*" Regel 18a berichtet der Vorstand zumindestens einmal jährlich über die Vorkehrungen zur Bekämpfung der Korruption im Unternehmen. Gemäß *Schopper* ist diese Regel so zu interpretieren, dass der Vorstand der Konzernmutter dem Aufsichtsrat über Vorkehrungen zur Bekämpfung von Korruption in allen nachgeordneten Konzernunternehmen zu berichten hat. Die Festlegung und jede grundlegende Änderung der Strategie zur Korruptionsbekämpfung im Gesamtkonzern wäre, seines Erachtens, ein Grundsatz der Geschäftspolitik. [68]

Nach der C-Regel 70 beschreibt der Vorstand im Konzernlagebericht die wesentlichen eingesetzten Risikomanagementinstrumente in Bezug auf nicht-finanzielle Risiken.

[67] *Petsche/Mair*, Handbuch Compliance³ 30
[68] *Schopper* in *Kalss* in *Kalss/ Torggler*, Beiträge zum 4. Unternehmensrechtstag (2016) 61

Noch deutlicher und daher als materiell-rechtliche Grundlage klar herangezogen werden kann der deutsche Corporate Governance Kodex. Dieser befasst sich explizit mit Compliance und legt dort unter anderem folgendes fest:

- Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der Strategie, der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance
- 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)
- Der Aufsichtsrat soll einen Prüfungsausschuss (Audit Committee) einrichten, der sich – falls kein anderer Ausschuss damit betraut ist - mit Compliance befasst

Als weiteres Grundprinzip legt der deutsche Corporate Governance Kodex fest, dass sich gute Unternehmensführung durch legales und ethisch fundiertes, eigenverantwortliches Verhalten auszeichnet. Demnach sollen Unternehmen die Grundzüge des Compliance-Management-Systems offenlegen, damit sich Investoren, aber auch die interessierte Öffentlichkeit, ein eigenes Bild von den Compliance Anstrengungen des Unternehmens machen können. Ziel ist eine Stärkung des Vertrauens in eine verantwortungsvolle Unternehmensführung. Im Sinne eines „Best Practice“ Compliance Systems soll den Beschäftigten auf geeignete Weise die Möglichkeit eingeräumt werden, geschützt Hinweise auf Rechtsverstöße im Unternehmen zu geben.[69]

E. Folge aus materiellrechtlichen Compliance Bestimmungen

Wie bereits ausgeführt, bestehen auf bestimmte Materien beschränkte Compliance-Regelungen, wobei in der vorliegenden Arbeit die einschlägigen Bestimmungen zur Geldwäscheprävention als auch jene im Bundesvergabegesetz und im Versicherungsaufsichtsgesetz näher dargestellt werden.

So wird für Rechtsanwälte in § 8a Abs. 2 RAO die gegebenenfalls bestehende Pflicht zur Bestellung eines Compliance-Beauftragten ausdrücklich verankert. Auch für Immobilienmakler ist gesetzlich geregelt (§ 365n1 Abs. 4 GewO), dass sich eine Verpflichtung für die Bestellung eines, auf Führungsebene angesiedelten, Beauftragten

[69] Arbeitsunterlage Corporate Compliance Officer Lehrgang, “Governance & Compliance”

ergeben kann, welcher für die Implementierung und Sicherstellung der Compliance-Maßnahmen Sorge zu tragen hat.

Zusätzlich zur Regelung zur Bestellung einer Person zum Compliance-Beauftragten, verlangen die hier einschlägigen Normen die Implementierung von Compliance-Maßnahmen, also das Einhalten von Sorgfaltspflichten wie etwa die Erstellung und laufende Verbesserung der Risikoanalyse, welche indirekt sehr wohl zur Einführung eines Compliance-Management-Systems verwenden werden können.

F. Folge des Durchführens eine Risikoanalyse beziehungsweise aus anderen Überlegungen

Wie von *Reich-Rohrwig* richtigerweise herausgearbeitet, können nach Lage des Einzelfalls Rechtsvorschriften außerhalb des Aktiengesetzes sowie betriebswirtschaftliche Abwägungsentscheidungen das jeweilige Unternehmen so stark betreffen oder verpflichten, dass die Einrichtung einer Compliance-Organisation aus Sicht des allgemeinen Sorgfaltsmaßstabes unumgänglich ist.

Als Beispiele führt jener Fälle an, in welchen Unternehmen von öffentlichen Auftragsvergaben abhängig sind und schon aus einzelnen Compliance-Verstößen der mögliche Ausschluss von öffentlichen Vergaben droht.

Seiner Ansicht nach kann gleiches gelten, wenn ausländische Rechtsvorschriften ein konzernweites Compliance-System notwendig machen oder wesentliche Geschäftspartner die Einführung eines solchen zur Geschäftsbedingung machen, allenfalls sogar vertragliche Konsequenzen an das Bestehen eines solchen knüpfen.[70] Bei Unternehmen gewisser Größe wird die Einrichtung eines Compliance-Management-Systems zunehmend als Standard empfunden und es existieren zahlreiche Best-Practice Modelle von Compliance-Systemen.[71]

Wie bereits dargestellt, argumentiert *Jaufer* mit den im Unternehmens- und Gesellschaftsrecht bestehenden Insolvenzprophylaxebestimmungen Corporate Compliance. So führt jener aus, dass die seit Jahrzehnten bestehenden Insolvenzprophylaxevbestimmungen wesentliche Elemente einer ordnungsgemäßen Corporate Compliance darstellen.[72]

[70] J. *Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II[6] § 82 Rz 39
[71] J. *Reich-Rohrwig/Zimmermann* in *Artmann/Karollus,* AktG II[6] § 82 Rz 42
[72] *Jaufer* in SWK 19/2011, W 41

Weitere wesentliche Aspekte beziehungsweise Gründe für die Einführung eines Compliance-Management-Systems sind meiner Einschätzung zufolge: Die Vermeidung eines Reputationsschadens im Falle eines Compliance-Verstoßes sowie die Erlangung beziehungsweise weitere Aufrechterhaltung von Compliance-Zertifizierungen, welche wiederum als Wettbewerbsvorteil gegenüber anderen, nicht-zertifizierten Unternehmen dienen können.

Darüber hinaus kann sich die Einrichtung eines Compliance-Management-Systems als Konsequenz des Durchführens einer Risikoanalyse ergeben. Eine Risikoanalyse wird zumeist im Rahmen des Risikomanagements durchgeführt. Es werden dabei gewisse Risikobereiche, darunter auch Compliance-Risiken, wie beispielsweise datenschutzrechtliche Vergehen beziehungsweise Betrugsrisiken im Unternehmen, identifiziert. Je nach Risiko-Appetit und gewählten Maßnahmen, kann die Risikolandkarte als Grundlage für die Einführung eines Compliance-Management-Systems herangezogen werden, welches wiederum die Einführung von Maßnahmen vorsieht, um (Compliance-)Risiken in den Risikobereichen vorzubeugen oder zumindestens deren Eintrittswahrscheinlichkeit zu verringern.

G. Entwicklungen auf europäischer Ebene

Darüber hinaus wird an dieser Stelle auf europaweite legistische Entwicklungen zu bestimmten Themen, welche typischerweise Compliance zugeordnet werden, hingewiesen.

Allen voran die von der EU erlassene Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden - (EU) 2019/1937 – die sogenannte „Whistleblowing Richtlinie“, welche am 23.10.2019 erlassen und bis Ende 2021 von den EU-Mitgliedsstaaten in nationales Recht umzusetzen war. Zum Zeitpunkt des Verfassens der vorliegenden Arbeit hat die Mehrheit der europäischen Mitgliedsstaaten die Richtlinie noch nicht in nationales Recht implementiert.

Die Richtlinie sieht im Wesentlichen vor, dass Unternehmen ab einer gewissen Mindestgröße Systeme einrichten müssen, um Hinweise beziehungsweise Meldungen zu vermutetem Fehlverhalten in Compliance-Bereichen (wie zum Beispiel im Datenschutz, Produkthaftung) vertraulich entgegenzunehmen und diesen nachzukommen.

Im Zeitpunkt des Verfassens der vorliegenden Arbeit liegt für Österreich ein entsprechender Gesetzesentwurf vor. Das Bundesgesetz über das Verfahren und den Schutz bei Hinweisen auf Rechtsverletzungen in bestimmten Rechtsbereichen, kurz

„Whistleblowinggesetz“ (WbG), enthält detaillierte Regelungen unter anderem zur Einrichtung interner Hinweisgebersysteme als auch zum Schutz des Hinweisgebers vor allfälligen Repressalien.

Unternehmen, welche in den Anwendungsbereich des Whistleblowinggesetzes fallen, müssen Verfahren, Prozesse und Meldekanäle schaffen und einrichten, damit Meldungen, die in den Schutzbereich der Bestimmung fallen, entgegengenommen und bearbeitet werden können. Als weitere Folge müssen gegebenenfalls interne Untersuchungen durchgeführt werden. Sollte sich gemeldetes Fehlverhalten bestätigen, sind Prozesse zu implementieren, um weiteres Fehlverhalten zu verhindern.

Es ist davon auszugehen, dass die Einführung des Whistleblowinggesetzes bei vielen Unternehmen als Grundlage für die Konzeption und Einführung von Compliance-Management Systemen herangezogen werden wird.

H. Abgrenzung Compliance zu anderen (Kontroll-)Instanzen

1. Abgrenzung zum internen Kontrollsystem

In der Literatur ist eine Diskussion in der Literatur darüber ausgebrochen, ob und wenn ja, wie weit Compliance und das interne Kontrollsystem eine Deckungsgleichheit aufweisen.

Meines Erachtens ist der, der Literatur zu entnehmenden (hier vor allem *Reich-Rohrwig*) teilweisen Gleichsetzung vom Institut des internen Kontrollsystems und eines Compliance-Management-Systems nur bedingt zuzustimmen. Dies wiederum kann begründet werden mit den Ausführungen in facheinschlägiger Judikatur. Hier insbesondere hervorzuheben ist das sogenannte „Three Lines of Defense Model“, welches ein dreistufiges Sicherheits- und Verantwortlichkeitenmodell vorsieht. Nähere Ausführungen dazu finden sich weiter unten in diesem Kapitel. Von *Petsche/Larcher* wird das interne Kontrollsystem als gleichwertiges Element neben dem Compliance Management und dem Risiko Management dargestellt, welche zusammen mit der internen Revision das „House of Governance“ und damit die Corporate Governance darstellen.[73] Gemäß *Reich-Rohrwig* im ist der Begriff des internen Kontrollsystems in einem engen Sinn auszulegen: „*Wenngleich ein Internes Kontrollsystem und eine Interne Revision auf jeden Fall einzurichten sind, kann z.B. eine Pflicht zur Installierung eines Frühaufklärungssystems oder generell eines*

[73] *Petsche/Larcher* in *Petsche/Mair*, Handbuch Compliance³ 32

umfassenden Risikomanagement(systems) aus dem Gesetz nicht abgeleitet werden – insoweit ist die Textierung eindeutig.“[74]

Das Institut für Corporate Governance (ICG) in der deutschen Immobilienwirtschaft sieht vier Governance Elemente vor:

(1) Interne Revision

(2) Internes Kontrollsystem

(3) Compliance und

Die Trennung dieser Bereiche findet sich auch in dem „Three Lines of Defense Model” von COSO (= Committee of Sponsoring Organizations of the Treadway Commission). Dort wird in dem „Internal Control – Integrated Framework“ auf ein dreistufiges Modell abgestellt. Dabei bilden sogenannte „Management Controls“ sowie „Internal Control Measures“ die „1st line of defense“. In der „2nd line of defense“ finden sich – neben Abteilungen wie „Financial Control“, „Security“, „Quality“ und „Inspection“ – die Bereiche „Risk Management“ und „Compliance“. Auf der dritten Ebene („3rd line of defense“) findet sich Internal Audit.

Als, diesen drei Ebenen zugrundeliegende, Verantwortlichkeiten finden sich auf der ersten Ebene „*own and manage risk and control*“. Adressat sind die jeweils operativ tätigen Fachbereiche. Auf der zweiten Ebene – „*monitor risk and control in support of management*“ – sollen Risiko- und Compliance-Funktionen die identifizierten Risiken überwachen, und somit Management unterstützen. Die dritte Ebene, ausgeübt durch eine „Internal Audit“ Funktion, ist ausschließlich auf eine unabhängige Kontrolle ausgerichtet – „*provide independent assurance*“. Diese „assurance“ Funktion soll Management dabei unterstützen, die Effektivität der Risiko- und Kontrollmaßnahmen zu überwachen.

Aus dem „Three Lines of Defense Model” ergibt sich eindeutig die Unterscheidung zwischen internen Kontrollmaßnahmen, welche auf der ersten Ebene beim Fachbereich angesiedelt sind, und der Überprüfungsfunktion von, unter anderem, Compliance, welche auf der zweiten Ebene angesiedelt ist.[75]
Napokoj führt Überschneidungen zwischen Compliance und internem Kontrollsystem ins Treffen. Dies in Bezug auf die Ordnungsmäßigkeit, welche als eines der Ziele des internen Kontrollsystems angeführt wird. Der Begriff der Ordnungsmäßigkeit zielt dabei auf die

[74] *Reich-Rohrwig* in *Straube/Ratka/Rauter*, WK GmbHG § 25 Rz 16
[75] COSO –“Leveraging COSO across the three lines of defense” (coso-2015-3lod.pdf)

Einhaltung der Gesetze ab und ist Teil der Prüfungstätigkeit des internen Kontrollsystems. Aufgrund der Unabhängigkeit der Compliance-Organisation kommt *Napokoj* aber zum Schluss, dass Compliance nicht Teil des internen Kontrollsystems werden darf. Vielmehr sieht sie eine enge Kooperation zwischen den beiden Funktionen, in welcher laufend Informationen ausgetauscht werden und eine wechselseitige Beratung stattfindet. Weiters führt jene ins Treffen, dass die Compliance-Organisation Maßnahmen aufzeigen muss, die rechtliche Risiken beinhalten können. Das interne Kontrollsystem habe dies in Bezug auf die Sicherheit zu überprüfen. Das interne Kontrollsystem wiederum sei von Compliance zu überwachen, weil dieses selbst ein Compliance-Risiko darstellen könne. Dabei handle es sich nicht um ein Risiko aufgrund der Geschäftstätigkeit, sondern vielmehr um ein Kontrollrisiko.[76]

Gewissermaßen eine Anti-These zu der Ansicht, dass das interne Kontrollsystem zu großen Teilen nicht deckungsgleich mit dem Compliance-Management-System ist, liefern die materiellrechtlichen Bestimmungen zum internen Kontrollsystem im Versicherungsaufsichtsgesetz (nähere Ausführungen dazu unter Punkt III.C.), in welchen die Compliance-Funktion als Teil des internen Kontrollsystems angeführt wird.

2. Abgrenzung zum Risikomanagement

Zwischen Compliance und Risiko Management bestehen große Schnittmengen. Gemäß § 92 Abs 4a Z 2 AktG hat der Prüfungsausschuss des Aufsichtsrats die Wirksamkeit des Risikomanagements zu überwachen. Unter Risikomanagement werden dabei alle Maßnahmen verstanden, welche zur Erkennung von Entwicklungen dienen, die den Fortbestand des Unternehmens gefährden könnten.

Zwischen Compliance und Risikomanagement besteht eine Schnittmenge, weil insbesondere Compliance-Risiken von Risikomanagement erkannt werden müssen. Umgekehrt kann auch das Risiko-Management ein Compliance-Risiko darstellen.[77]

Neben diesen von *Napokoj* angeführten Überschneidungen ergibt sich, meines Erachtens auch eine große Schnittmenge durch die Arbeitsweise der beiden Funktionen. So besteht die Arbeit der Compliance-Organisationen zu einem großen Teil aus dem Erkennen und Identifizieren von (Compliance-)Risiken, welche dann entsprechend verringert und denen durch Präventiv- und Korrekturmaßnahmen entgegengewirkt werden soll.

[76] *E. Napokoj* in *Napokoj*, Risikominimierung durch Corporate Compliance (2010) Rz 44f mwN
[77] *E. Napokoj* in *Napokoj*, Risikominimierung Rz 48

Zwischen beiden Bereichen sollte ein regelmäßiger Austausch im Sinne eines Informationsaustausches und wechselseitiger Beratung sowie Abstimmung erfolgen.

3. Abgrenzung zur internen Revision

Die interne Revision wird oftmals als „Kontrolle von der Kontrolle“ bezeichnet und nimmt eine Überwachungsfunktion in der Organisation ein.

Napokoj sieht die Aufgabe von Compliance darin, die interne Revision in rechtlichen Fragen zu beraten, während die interne Revision die Compliance-Funktion bei der Ermittlung von Sachverhalten unterstützt. Die interne Revision überprüft auch die Compliance-Abteilung und macht erforderlichenfalls Vorschläge zu deren Verbesserung.

Des Weiteren unterstützt die Überwachungsfunktion der internen Revision die Tätigkeit der anderen Überwachungsfunktionen, sohin auch Compliance.[78]

Diese Ansicht deckt sich auch mit dem dreistufigen Modell nach COSO, welches die interne Revision als „3rd line of defence“ bezeichnet.

Nach dem „House of Corporate Governance“ bildet die interne Revision gewissermaßen die allumfassende Überwachungsfunktion, welche zusätzlich zum Compliance Management, dem Risiko Management und dem internen Kontrollsystem besteht.

Nach *Petsche/Larcher* soll die interne Revision vorwiegend die Unternehmensleitung in ihrer Kontrollfunktion unterstützen. Demnach kommt der internen Revision die Aufgabe zu, Unternehmensvorgänge auf ihre Ordnungsmäßigkeit zu prüfen und Unwirtschaftlichkeiten, Unregelmäßigkeiten und Manipulationen aufzudecken. Dabei muss die interne Revision unabhängig agieren und zugleich umfangreiche Informationsrechte besitzen.[79]

[78] *E. Napokoj* in *Napokoj*, Risikominimierung Rz 46
[79] *Petsche/Larcher* in *Petsche/Mair*, Handbuch Compliance³ 10

V. Hauptbestandteile eines Compliance-Management-Systems

Bei der Diskussion über die Einführung von Compliance-Management-Systemen relevant ist der Umstand, dass es keine gesetzliche Regelung beziehungsweise eine allgemeingültige Antwort dazu gibt, wie ein solches System auszusehen hat beziehungsweise gestaltet sein sollte.

So gibt es einzelne Anhaltspunkte in den einschlägigen Bestimmungen für Compliance-relevante Themenbereiche, wie beispielsweise im Versicherungsaufsichtsgesetz. Diese Bestimmungen können als Richtschnur für die Implementierung solcher Systeme herangezogen werden, sind aber zu spezifisch auf den jeweiligen Geschäftszweig (z.B. Versicherungsunternehmen) zugeschnitten, um als allgemeiner Maßstab zu dienen.

In der Praxis bedeutend sind die Leitlinien und Standards („Normen"), die von Normungsinstituten beziehungsweise einschlägigen Verbänden herausgegeben werden. Zu nennen ist hier vor allem die ISO 37301, welche eine Leitlinie für die Zertifizierung von Compliance-Management Systemen bildet (die ISO 37301 ersetzt die ISO 19600). Gemäß dieser Bestimmung sollten Compliance-Management-Systeme auf den Grundsätzen der guten Unternehmensführung, der Verhältnismäßigkeit, der Integrität, der Transparenz, der Rechenschaftspflicht und der Nachhaltigkeit beruhen. Es sind folgende Themenblöcke adressiert:

1) Bewertung der Risiken (Risikoanalyse)
2) Führung
3) Systemische Steuerungs- und Kontrollmechanismen
4) Training und Kommunikation
5) Monitoring, interne Audits und Reaktion

Die Norm ISO 37301 ist so konzipiert, dass sie auf alle Organisationsformen angewendet werden kann, wobei die Umsetzung je nach Kontext, Art und Komplexität der Aktivitäten und dem Zweck der Organisation unterschiedlich ist. Für ein effektives Compliance-Management-System nach ISO 37301 in jedem Fall zu implementieren sind zum einen ein Hinweisgebersystem („*raising concern*"), welche Meldungen über versuchte, vermutete oder tatsächliche Verstöße gegen Compliance-Richtlinien oder Verpflichtungen fördern und ermöglichen sowie den Hinweisgeber vor Vergeltungsmaßnahmen schützen soll.

Zum anderen muss ein Prozess eingerichtet und aufrechterhalten werden, um Berichte über vermutete oder tatsächliche Verstöße zu bewerten, zu untersuchen und abzuschließen: „Untersuchungen – *investigation process*“.[80]

Zusätzlich hervorgehoben wird die Bedeutung der Compliance Kultur im Unternehmen (Förderung regelkonformer Handlungen durch die oberste Unternehmensleitung) sowie zusätzliche operative Maßnahmen, welche sich nach den Ergebnissen der Compliance-Risiko-Analyse ergeben. Des Weiteren wird ausdrücklich der kontinuierliche, strukturierte Verbesserungsprozess hervorgehoben. Zusätzlich erfordert die Norm Schulungs- und Kommunikationsmaßnahmen, Überprüfungen, interne Audits, Managementbewertungen sowie Korrektur- und Verbesserungsmaßnahmen.[81]

Eingebettet in den Standards sind dabei wesentliche Anforderungen, welche für die Einrichtung eines effektiven und effizienten Compliance-Management-Systems gelten. Die Grundsätze werden dabei abstrakt beschrieben und umfassen – unter anderem – folgende Themenbereiche:

- „Tone from the top“
(Sicherstellen, dass das oberste Management die Compliance-Organisation unterstützt)
- Risikoanalyse
- Kommunikation und Schulungen
- Geschäftspartnerprüfungen
- Einführung von Kontrollmechanismen
- Überwachung und Untersuchung von Fällen der Nichteinhaltung
- Einführung eines effektiven Whistleblowing-Systems und Schutz des Hinweisgebers

Ein weiterer wichtiger Standard in diesem Bereich ist, der vom deutschen Berufsverband, dem Institut der deutschen Wirtschaftsprüfer, herausgegebene Standard IDW PS 980. Der Prüfstandard ist 2011 seitens des Instituts der Deutschen Wirtschaftsprüfer eingeführt worden, welcher erstmals Grundsätze für die ordnungsgemäße Prüfung von Compliance-Management-Systemen einführt. Nach den Vorgaben des IDW Prüfstandard 980 weist ein angemessenes Compliance-Management-System folgende Grundelemente auf, welche miteinander in Wechselwirkung stehen:

[80] Vgl. Compliance Praxis 3/2020 “Aus ISO 19600 wird ISO 373001“
[81] Vgl. Compliance Praxis 3/2020 “Aus ISO 19600 wird ISO 373001“

- Compliance-Kultur

- Compliance-Ziele

- Compliance-Organisation

- Compliance-Risiken

- Compliance-Programm

- Compliance-Kommunikation

- Compliance-Überwachung und Verbesserung[82]

Gemein ist den Standards und Normen, dass jene nicht rechtsverbindlich sind. Eine gewisse Form der „Rechtsverbindlichkeit" für das jeweilige Unternehmen kann lediglich über die Implementierung in entsprechende Compliance-Management-Systeme beziehungsweise als unternehmensinterne Richtlinien oder Weisungen entstehen. [83]

Für die Einführung von Compliance-Management-Systemen in Unternehmen relevant sind auch die Richtlinien und Handlungsanweisungen („Guidelines") zu internationalen Rechtsakten, wie zum englischen Korruptionsrecht - UK Bribery Act sowie dem US-amerikanischen Korruptionsrecht - dem US Foreign Corrupt Practices Act. Hierbei besonders die von jenen getroffenen Aussagen zur Gestaltung eines effektiven Compliance-Management-Systems. Jene Rechtsakte und die praktische Implementierung der darauf basierenden Systeme dienen als internationale Best Practices.

Als wesentliche Standards im anglo-amerikanischen Bereich dienen vor allem:

- US Sentencing Guideline Manual (USSG's 7 elements of an effective compliance program)

- 13 good practices by the OECD on internal controls, ethics and compliance

- UK's 6 principles for "adequate procedures"

- Transparency International: Business principles for countering bribery

Konkret sieht das US Sentencing Guideline Manual Strafmilderungen für Compliance-Systeme vor, welche „*reasonable designed, implemented and enforced*" sind. Laut Guideline Manual sind demnach sieben Punkte angeführt, welche von den Unternehmen

[82] *Kretschmer* in *Petsche/Mair*, Handbuch Compliance³ 75
[83] *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus*, AktG II⁶ § 82 Rz 43

als Mindeststandards eingeführt werden müssen. So haben Unternehmen unter anderem über etablierte Compliance-Standards und Compliance-Verfahrensweisen zu verfügen, welche geeignet sein müssen, die Gefahr kriminellen Verhaltens zu reduzieren. Jene sind den Mitarbeitern zu vermitteln, beispielsweise durch verpflichtende Trainingsprogramme.

Die Erreichung der Compliance-Standards ist durch permanentes „monitoring" und „auditing" sicherzustellen, um die Aufdeckung von Straftaten zu erreichen. Weiters sind die Compliance-Standards durch disziplinarische Maßnahmen nachhaltig durchzusetzen. Einige Punkte in dem Programm erscheinen im heimischen System eher ungewöhnlich. So besagt eine Regel, Mitarbeitern, von denen bekannt ist oder bekannt sein müsste, dass sie kriminelle Neigungen haben, dürfe keine substanzielle Ermessensverantwortung eingeräumt werden.

In Großbritannien hat die Kartellrechtsbehörde eine Richtlinie herausgegeben, welche auch Maßnahmen umfasst, die bei Unternehmen zu einer Strafreduzierung führen können. Darunter finden sich Bestimmungen, wonach Compliance-Programme aktiv eingeführt werden müssen und der sichtbaren und dauerhaften Unterstützung des Senior Managements bedürfen, welches die Einhaltung der Compliance überwacht. Zusätzlich besteht die Verpflichtung zur Durchführung von Trainings und eine regelmäßige Evaluierung des Programms.[84]

Ausgehend von den Standards, haben sich folgende drei Themenbereiche im Hinblick auf Compliance-Management-Systeme herauskristallisiert:

1) „Vorbeugen" („Prevent")
2) „Erkennen" („Detect")
3) „Reagieren" („React")

Wie von *J. Reich-Rohrwig*/*Zimmermann* richtigerweise ausgeführt, betonen die Vorschriften hierbei selbst, sie seien als allgemeine Prinzipien hochgradig und für jedes Unternehmen individuell ausgestaltungsbedürftig. Zutreffenderweise stellen sie daher nur eine Richtschnur dar. Vor diesem Hintergrund sind auch Zertifizierungen von Compliance-Systemen nur bedingt geeignet, eine generelle Vermutung für ein in allen Belangen adäquates Legalitätskontrollsystem zu begründen. Insbesondere die Überprüfung der Wirksamkeit des Compliance-Systems als „Knackpunkt"einer effektiven Legalitätskontrollfunktion ist bei Compliance-Zertifizierungen, die hier auf

[84] *E. Napokoj* in *Napokoj*, Risikominimierung Rz 50f

stichprobenhafte Untersuchungen angewiesen sind, nicht lückenlos möglich. Allerdings können im Zuge der Zertifizierungsverfahren vorgenommen Überprüfungen des Compliance-Management-Systems ein wichtiges Mittel für den Vorstand sein, nachzuweisen, dass jener seinen Kontroll- und Überwachungspflichten hinreichend nachgekommen ist. Dies natürlich nur dann, wenn dem Vorstand keine Anhaltspunkte dafür vorliegen, dass das Compliance-Management-System unwirksam ist. [85]

Ein Compliance-Management-System setzt sich, gemäß den hier erwähnten, von unabhängigen Instituten entwickelten Standards – hier insbesondere erwähnenswert der IDW PS 980 und die ISO 37301 – typischerweise aus den folgenden Hauptkomponenten zusammen:

- Anforderungen (Analyse des Unternehmensumfelds, Strategie, Pflichtendelegation etc.)

- Risikoanalysen (Analyse der unternehmensspezifischen Risiken etc.)

- Organisation (Organisations-Richtlinie, Definition der Ansprechpartner/Compliance Officer etc.)

- Prozesse (Compliance-Richtlinien, z.B. Verhaltenskodex, Anti-Korruption, Geldwäsche, Kartellrecht)

- Integration (Anpassung bzw. Einführung von Richtlinien, Kontrollen im Tagesgeschäft, Kommunikation, Schulungen etc.)

[85] *J. Reich-Rohrwig/Zimmermann* in *Artmann/Karollus*, AktG II[6] § 82 Rz 43

Literaturverzeichnis

Petsche/Mair, Handbuch Compliance, 3 Auflage

Sartor, Praxisleitfaden Compliance, 2. Auflage

Peter Lewisch, Zauberwort Compliance? Wien, 2012

Kalss/ Torggler, Beiträge zum 4. Unternehmensrechtstag (2016)

Napokoj, Risikominimierung durch Corporate Compliance (2010)

Lewisch/Fister/Weilguni, Verwaltungsstrafgesetz, VStG, 2. Auflage (Stand: 1.5.2017)

Artmann/Karollus, Aktiengesetz, Kommentar zum Aktiengesetz, 6. Auflage (Stand: 1.9.2019)

Straube/Ratka/Rauter, Wiener Kommentar zum GmbHG-Gesetz (Stand: 1.9.2021)

Höpfel/Ratz, Wiener Kommentar zum Strafgesetzbuch (Stand: 1.12.2021)

Gruber/Paliege-Barfuß, Gewerbeordnung – GewO (Stand: 1.9.2020)

Gölles, Bundesvergabegesetz, BVergG 2018 (Stand: 1.10.2020)

Moick/Gföhler, Bundesvergabegesetz, BVergG 2018, Höchstgerichtliche Judikatur in Leitsätzen (Stand: 1.3.2021)

Jaufer in SWK 19/2011, W 41

Compliance Praxis (unterschiedliche Fachbeiträge)