WEBER & CO.
RECHTSANWÄLTE

12. BKMS Experience Days

EU WB-RL: Ändert die neue Whistleblowing Richtlinie etwas an der haftungsrechtlichen Perspektive?

Dr. Katharina Kitzberger
15. September 2021

Inhalt

Einleitung
Compliance Risk Assessment

Einleitung I
Was ist Compliance?

Abbildung 1: https://www.ruhlamat.com/de/unternehmen/compliance-richtlinie (24.3.2020)

Einleitung II
Begriff „Compliance“

Der Begriff „Compliance“ bezeichnet die Gesamtheit aller zumutbaren Maßnahmen, die das regelkonforme Verhalten eines Unternehmens, seiner Leistungs- und Aufsichtsorgane sowie seiner Organisationsmitglieder im Hinblick auf alle gesetzlichen Ge- und Verbote begründen.

(Petsche/Larcher, Was ist Compliance?, in *Petsche/Mair*, Handbuch Compliance[3] (2019) 33*)*

Aber: Welche Maßnahmen sind zumutbar? Und: Was sind die relevanten gesetzlichen Ge- und Verbote?

Einleitung III
Der Weg zum Ziel: Compliance Risk Assessment

Zweck eines Compliance Risk Assessment ist die Ermittlung der bestehenden Unternehmensrisiken. Auf Basis des Ergebnisses des Compliance Risk Assessment soll in weiterer Folge ein (adäquates) Compliance Management System (CMS) aufgebaut werden.

- Es gibt keine (wenige?) gesetzliche Vorgaben, wie ein CMS auszusehen hat;
- Es gibt keine gesetzlichen Vorgaben, wie ein Compliance Risk Assessment auszusehen hat;
- Das Compliance Risk Assessment ist ein integraler Bestandteil des gesamten Compliance Management Prozesses.
- Übliche Zertifizierungen verlangen einen risikobasierten Ansatz bei der Erstellung des CMS.

Einleitung IV
Identifizierung und Klassifizierung der Risiken

Identifizierung der Risiken

- Anwendbare Rechtsnormen, Branche?, unternehmensinterner Aufbau, Unternehmenskultur, Größe des Unternehmens, Organisationsstruktur, insbesondere Einkauf/Verkauf;

Teilnehmer des Identifikationsprozesses?

Klassifizierung

- Risk-owner: Zurechnung eines bestimmten Risikos;
- Risikoarten: unmittelbare Haftung des Unternehmens/der Organe, unmittelbare Schädigung des Unternehmensvermögens, mittelbare Vermögens- und Reputationsschäden;

Einleitung V
Risikoanalyse

- Erforschung der Ursachen der Risiken
- Compliance Risiken sind Verhaltensrisiken > Verhaltensanalyse: Das Verhalten der Mitarbeiter soll geändert werden.

Relevanz eines Risikos: Potenzielles Ausmaß eines Risikos im Verhältnis zur Wahrscheinlichkeit, dass das Risiko eintritt.

- Wahrscheinlichkeit des Eintritts: Interne (zB Komplexität der Unternehmensorganisation, Anzahl der Fälle in der Vergangenheit) und externe (zB Tätigkeit in korruptionsanfälligem Staat) Faktoren.
- Ausmaß des befürchteten Risikos: Quantitative (Höhe des Vermögensschadens) und qualitative Komponente.

Einleitung VI
Risikobewertung I

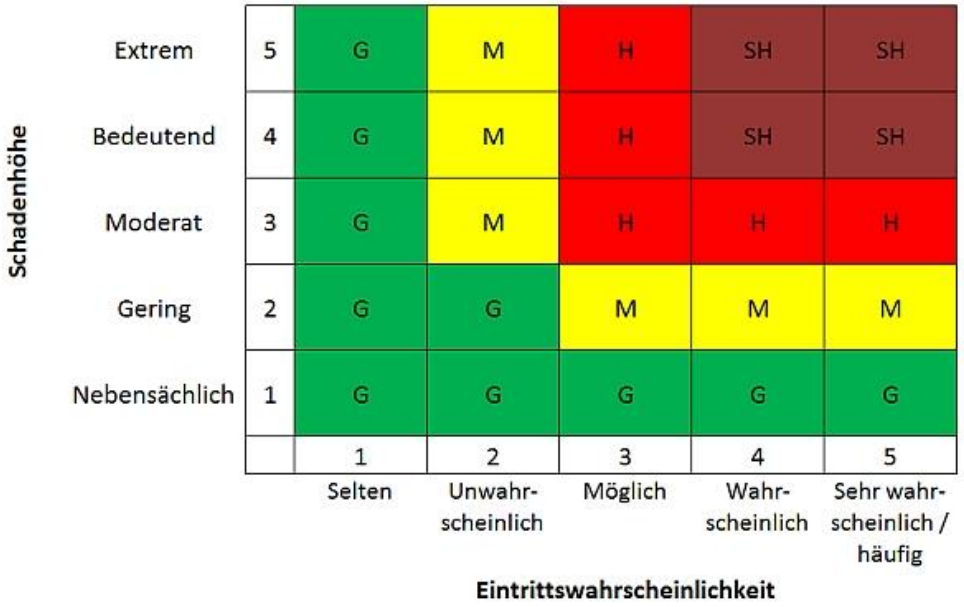

Abbildung 2: https://www.compliance-manager.net/fachartikel/herangehensweisen-das-compliance-risikomanagement-1774965701 (24.3.2021)

Einleitung VII
Risikobewertung II

- Risikobewertung dient dazu, jene Risiken aufzudecken, die die Einleitung einer Compliance-Maßnahme erfordern.
- Gleichzeitig soll eine Priorisierung der einzelnen Compliance-Maßnahmen erfolgen.
- Mit Hilfe einer Matrix können die identifizierten und analysierten Risiken je nach Eintrittswahrscheinlichkeit und befürchtetes Schädigungsausmaß eingetragen werden.

- Dokumentation der Risikobewertung
- Regelmäßige Überprüfung der Risikobewertung

Aktueller Rechtsrahmen bei der Umsetzung eines Compliance Management Systems

Rechtsrahmen AT I
Pflicht oder Ermessen?

- In Österreich gibt es bis dato keine ausdrückliche gesetzliche Pflicht zur Implementierung eines Compliance Management Systems (CMS) für Vorstände/Geschäftsführer
    - Ausnahme sind branchenspezifische gesetzliche Anforderungen, zB für Banken, Wertpapierdienstleistungsunternehmen und Versicherungen (§99g BWG, §26 Abs 2 Z 1 WAG 2018; §119 Abs 4 BörseG 2018) – kein Ermessen, ob ein System einzurichten ist, sondern lediglich bei der Ausgestaltung
    - Verpflichtung zur Implementierung eines internen Kontrollsystems (IKS, § 22 GmbHG, § 82 AktG)
- Geschäftsführung/Vorstand: Haben die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters einzuhalten (§ 25 GmbHG/§§ 70, 84 AktG) / Business Judgement Rule (BJR)
    - Grundsätzliche Entscheidung über CMS: Gesamtvorstand; Ressortverteilung für Bereich Compliance zulässig, beseitigt aber Gesamtverantwortung nicht zur Gänze!

Rechtsrahmen AT II
Pflicht oder Ermessen?

- Auch im österreichischen Corporate Governance Kodex gibt es bis dato keine ausdrückliche gesetzliche Pflicht zur Implementierung eines CMS
    - Vorstand trifft geeignete Vorkehrungen zur Sicherstellung der Einhaltung der für das Unternehmen relevante Gesetze;
    - Der Vorstand berichtet dem Aufsichtsrat mindestens einmal jährlich über die Vorkehrungen zur Bekämpfung von Korruption im Unternehmen;
    - Weiters sind diverse erweise auf die Einrichtung eines Risikomanagementsystems enthalten.

Rechtsrahmen AT III
Pflicht oder Ermessen?

- Österreichisches Verbandsverantwortlichkeitsgesetz (Strafrecht für Unternehmen)
  - Ein Unternehmen ist für eine Straftat verantwortlich, wenn (i) die Tat zu seinen Gunsten begangen worden ist oder (ii) durch die Tat Pflichten verletzt worden sind, die das Unternehmen betreffen.
  - Haftung für Entscheidungsträger: wenn der Entscheidungsträger die Tat rechtswidrig und schuldhaft begangen hat.
  - Haftung für Mitarbeiter nur, wenn
    - (i) der Mitarbeiter rechtwidrig gehandelt hat und der notwendige Vorsatz beim Mitarbeiter erfüllt ist und
    - (ii) die Begehung der Tat dadurch ermöglicht oder wesentlich erleichtert wurde, dass Entscheidungsträger die nach den Umständen gebotene und zumutbare Sorgfalt außer acht gelassen haben, insbesondere indem sie wesentliche technische, organisatorische oder personelle Maßnahmen zur Verhinderung solcher Taten unterlassen haben (CMS).
  - Die Implementierung eines CMS kann daher die Strafbarkeit eines Unternehmens verhindern.

Rechtsrahmen DE I
Pflicht oder Ermessen?

- Auch in Deutschland gibt es im dAktG/dGmbHG keine ausdrückliche gesetzliche Pflicht zur Implementierung eines CMS für Vorstände/Geschäftsführer;
    - Ausnahme: Sondergesetze, wie zB KWG, VAG oder WpHG (samt Rundschreiben)
    - Legalitätspflicht: Pflicht zur Einhaltung sämtlicher Rechtsvorschriften, die das Unternehmen treffen (im Außenverhältnis)
    - Legalitätskontrollpflicht: Pflicht, für die Einhaltung des Rechts durch Dritte, dh Unternehmensangehörige zu sorgen
    - Aktienrechtliche Compliance-Verantwortung ist aus der allgemeinen Leitungssorgfalt der Vorstandsmitglieder gem §§ 76 I und 93 I dAktG abzuleiten (andere Lehrmeinungen: Einzelanalogie zu § 91 II dAktG oder Gesamtanalogie zu Compliance-Regeln in verschiedenen Materiengesetzen)
    - Grundsätzliche Entscheidung über CMS: Gesamtvorstand (delegationsfeindlich); Ressortverteilung für Bereich Compliance zulässig, beseitigt aber Gesamtverantwortung nicht zur Gänze (Überwachungspflicht bzw ggf auch Interventionspflicht)!

WEBER & CO.
RECHTSANWÄLTE

Rechtsrahmen DE II
Pflicht oder Ermessen?

- Der deutsche Corporate Governance Kodex kennt bereits seit 2007 den Begriff der „Compliance“; seit 2017 wird die Implementierung eines CMS empfohlen und auch auf die Wichtigkeit eines Hinweisgebersystems hingewiesen.
    - Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der internen Richtlinien zu sorgen und wirkt auf deren Beachtung im Unternehmen hin (Compliance)
    - Der Vorstand soll für ein an der Risikolage des Unternehmens ausgerichtetes Compliance Management System sorgen und dessen Grundzüge offenlegen. Beschäftigten soll auf geeignete Weise die Möglichkeit eingeräumt werden, geschützt Hinweise auf Rechtsverstöße im Unternehmen zu geben; auch Dritten sollte diese Möglichkeit eingeräumt werden.

Rechtsrahmen DE III
Pflicht oder Ermessen?

- Ordnungswidrigkeitengesetz (künftig auch Verbandssanktionengesetz?):
  - Geldbuße gegen juristische Personen und Personenvereinigungen, wenn eine Leitungsperson eine Straftat oder Ordnungswidrigkeit begangen hat, durch die Pflichten des Unternehmens verletzt wurden oder durch die das Unternehmen bereichert wurde oder werden sollte (§ 30 OWiG).
  - Eine Ordnungswidrigkeit begeht, wer als Inhaber eines Unternehmens diejenigen Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Unternehmen Zuwiderhandlungen gegen solche straf- oder bußgeldbewehrte Pflichten, die nicht unmittelbar an den Inhaber des Unternehmens adressiert sind, aber einen gewissen Unternehmensbezug haben (§ 130 OWiG).

Rechtsrahmen
Haftung I

- Siemens Neubürger-Urteil (LG München, 10.12.2013 zu 5 HKO 1387/10)
  - System schwarzer Kassen, System von Scheinberaterverträgen für Korruptionszahlungen; Bußgeldbescheide gegen Siemens AG;
  - Haftung eines Vorstandes wegen mangelnder Umsetzung eines geeigneten CMS (§ 93 dAktG); Schadenersatz in Höhe von EUR 15 Mio
  - Anforderungen an ein CMS: Ein Unternehmen muss derart organisiert werden, dass Gesetzesverletzungen nicht stattfinden
  - Keine Haftung des Vorstandes, wenn dieser eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation einrichtet
  - Keine Rechtfertigung wegen „Nichtkennens“ der Vorgänge im eigenen Geschäfts- oder Verantwortungsbereich des Vorstands; keine Rechtfertigung wegen Nichtdurchsetzen-könnens im Gesamtvorstand

Rechtsrahmen
Haftung II

Notwendige Sachkenntnis

- Ein Vertretungsorgan, das selbst nicht über die erforderliche Sachkunde verfügt, muss einen fachlich qualifizierten Berufsträger unter Offenlegung der notwendigen Unterlagen beiziehen und die erteilte (Rechts)auskunft einer sorgfältigen Plausibilitätskontrolle unterziehen.

  A-Tech Entscheidung: OGH, 30.8.2016 zu 6 Ob 198/15h / ISION Entscheidung: BGH, NZG 2011, 1271

Notwendige Sachkenntnis bei der Ausgestaltung eines CMS?

- Kein „*one size fits all*" Konzept: Entscheidung über die Implementierung eines CMS soll auf Basis von angemessenen Informationen (BJR) ergehen
- Kriterien: Art, Größe, Organisationsstruktur, Risikopotential (zB Vertriebstätigkeit), regulatorisches Umfeld des Unternehmens – Compliance Risk Assessment!

Exkurs: Umsetzung der EU Whistleblowing Richtlinie (EU WB-RL)

WEBER & CO.
RECHTSANWÄLTE

EU WB-RL I
Umsetzung ins nationale Recht

- EU WB-RL wurde am 26.11.2019 im Amtsblatt der Europäischen Union veröffentlicht und ist bis zum 17.12.2021 vom Gesetzgeber in nationales Recht umzusetzen
- Spielraum bei der Umsetzung
- Österreich: Die konkrete Umsetzung ist noch offen (zB ob Anwendungsbereich auf Verstöße gegen nationales Recht ausgeweitet wird; ob eigenes Gesetz oder Umsetzung in diversen Gesetzen); ein Gesetzesentwurf soll im Herbst ins Parlament kommen.
- Deutschland: Hinweisgeberschutzgesetz wurde bereits Ende 2020 vom deutschen Justizministerium veröffentlicht; Gesetzesentwurf wurde im April 2021 allerdings gekippt, keine Einigung in der Koalition.

EU WB-RL II
Ausgestaltung des Hinweisgebersystems

- Meldekanäle, die Vertraulichkeit der Identität des Whistleblowers wahren
  - keine Verpflichtung für anonyme Meldekanäle
  - schriftliche und/oder mündliche Meldungsübermittlung
  - physische Zusammenkunft mit zuständiger Person/Dienststelle
  - kein Zugriff durch unbefugte Personen
- Festlegung von Zuständigkeiten für Folgemaßnahmen
  - darf gleich sein mit jener Person, die Meldungen entgegennimmt
- Bestätigung über Eingang der Meldung binnen 7 Tagen, Rückmeldung binnen 3 Monaten über Folgemaßnahmen (zB Veranlassung interner Ermittlungen, Weitergabe an Behörde, Einstellung der Verfolgung)
- Klar strukturierter Meldeprozess sowie Information, wann und unter welchen Bedingungen externe Meldung erfolgen kann

EU WB-RL III
Schutz für Whistleblower

- Bedingungen (Art 13 EU-WB-RL)
  - wenn der Whistleblower „[…] *hinreichenden Grund zu der Annahme hat, dass die von ihm gemeldeten Informationen zum Zeitpunkt ihrer Übermittlung der Wahrheit entsprachen und in den Anwendungsbereich dieser Richtlinie fallen "*
  - sensible Informationen, die zB unter Anwaltsgeheimnis oder ärztliche Verschwiegenheitspflicht fallen, dürfen nicht verbreitet werden (Art 26 WB-RL)
  - dreigliedriges System: interne Meldung – externe Meldung an Behörde – Öffentlichkeit, Medien

    Schutz für direkte öffentliche Meldung nur, wenn Grund zur Annahme der Gefahr für öffentliches Interesse / Risiko irreversibler Schäden bestand oder eine erfolglose Inanspruchnahme der internen oder behördlichen Hinweisgebersysteme voranging
- Schutz gegen Repressalien
- Schutz der in der Meldung beschuldigten Personen (Art 16 WB-RL)
- Schutz gegen jP, die Meldungen verhindern

Ausblick: Neuerungen aus haftungsrechtlicher Perspektive

Ausblick I
Bleibt alles anders?

Was bleibt

- Grundsätzlich breites Organisationsermessen des Vorstandes / Geschäftsleitung bei der Errichtung des CMS: Art, Größe und Organisation des Unternehmens, die zu beachtenden Vorschriften, geografische Präsenz und Verdachtsfälle in der Vergangenheit – Compliance Risk Assessment!
- Buchhaltung und Kassenführung: funktionsfähige Kontrollstrukturen
- Konkrete Verdachtsmomente: AAA: Aufklären, Abstellen, Ahnden
- Regelmäßige Überprüfung des CMS samt allfälligen Nachadjustierungen

Was sich ändert

- Künftig sind die EU WB-RL und deren Anforderungen bei der Einrichtung und Ausgestaltung eines Hinweisgebersystems zu beachten: es gibt kein Organisationsermessen mehr!

Ausblick II
Bleibt alles anders?

- Keine Universallösung, aber jedenfalls allgemeine organisatorische Anforderungen:
  - Bekenntnis zur Rechtstreue (tone from the top)
  - Klare Verantwortlichkeiten
  - Informationsfluss (zu Mitarbeitern – zB Code of Conduct; zu Compliance Officer – zB Information über Verstöße, über Meldungen von Verstößen etc)
  - Effektive Umsetzung des System (nur Papier ist geduldig)
  - Laufende Prüfung und ggf Aktualisierung des Systems

WEBER & CO.
RECHTSANWÄLTE

DR. KATHARINA KITZBERGER, B.A.
PARTNERIN

Zivil-, Unternehmens-
und Vertragsrecht, Haftungsrecht, Prozessführung,
Schiedsverfahren,
Compliance
T +43 1 427 2070
k.kitzberger@weber.co.at