Rechtswissen für IT-Manager, Berater und Verantwortliche

Business Judgement Rule – Compliance – IT-Compliance – IT-Governance

Walther Schmidt-Lademann

Rechtsanwalt

München 26. Januar 2012

Rechtswissen für Entscheider, Berater und Verantwortungsträger

Die Gefahr von Rechts- und Regelverletzungen wird für Unternehmen zum operationellen und und für Manager zum existenziellen Risiko.

> Schützen Sie sich durch adäquate **Compliance!**

Jede unternehmerische Tätigkeit hat ihre Risiken:

-Notwendigkeit zur Entscheidung in Unsicherheit

-Erwirtschaften risikoloser Gewinne ist nicht dauerhaft möglich

-Im Wettbewerb gibt es immer Gewinner und Verlierer

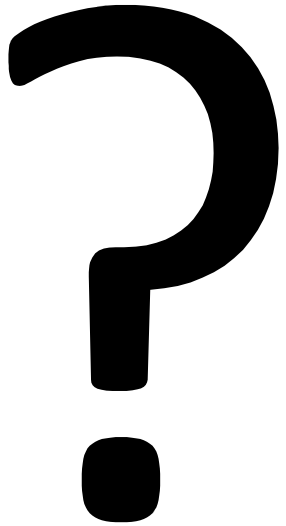
Richtiges Vorgehen bei der Entscheidung vermeidet Haftung:

- Erfahren Sie den Nutzen der **Business Judgement Rule** für effiziente und sichere Entscheidungen!
- Sehen Sie gleich wie Sie persönlicher Haftung entgehen!

Fragen

- Sind Sie
  - Geschäftsführer/Inhaber
  - Führungskraft mit Organisationsverantwortung
  - Berater/Freelancer
  - Techniker

- Was hat Ihr Interesse geweckt
  - Thema Rechtswissen allgemein
  - Business Judgement Rule
  - Compliance
  - Corporate Governance



Business Judgement Rule
Compliance und Corporate Governance

Business Judgement Rule - BJR

- Einstieg – Begriffe
- Vorgehen, Beispiel
- Nutzen

Compliance

- Begriff
- Inhalt
- Nutzen
- IT-Compliance

Corporate Governance - IT-Governance

Einstieg: Begriffe

- Aufgabe – Qua Funktion oder Delegation
- Verantwortung = Einstehen für die Konsequenzen
- Haftung –> Finanzielle und strafrechtliche Folgen
- Risiko: Persönlich und für das Unternehmen
- Management – Entscheidungen mit Konsequenzen
- Manager-Haftung - leichte Fahrlässigkeit reicht
- Beweislast für ordnungsgemäßes Handeln liegt bei der Geschäftsführung

BJR – Vorgehen

Haftungserleichterung bei unternehmerischen Entscheidungen durch Beachtung der BJR

I. Voraussetzungen - Vorgehen

- Unternehmerische Entscheidung oder Pflichtentscheidung?
- Fakten sammeln – so vollständig wie möglich
- Sichten – Ordnen
- Abwägung - Kriterien festlegen, gewichten…
- Entscheidung – zum Wohle des Unternehmens
- Dokumentation
- Umsetzung
- Kontrolle/Nachsteuern/neue Entscheidung

BJR Schematisch (Beispiel)

- Problem/Aufgabe
- Ist-Zustand
- Sollzustand/Ergebnis/Ziel
- Vorgehen – Alternativen: Fakten sammeln, sichten, ordnen
- Bewerten: Kriterien festlegen, gewichten (Zeit, Kosten (Anschaffung, Total Cost), Sicherheit, Eignung (Umfang der Zielerreichung), Skalierbarkeit…; SWOT-Analysen…
- Entscheiden – Ob; Was, Wie, Wer, Wann, Mittel - Also:
- Umsetzung – ggf. Plan, Milestones, Erfolgskriterien, Kontrollen
- Dokumentation
- Prüfung der Zielerreichung - Nachsteuern

Muster

Thema	Beschreibung	Datum
Anlass	Problem/Aufgabe	
Ist-Zustand		
Sollzustand/Ergebnis/Ziel		
Entscheidungsgrundlage Faktensammlung	Kurzfassung, Dokumentation s. Anlage	
Entscheidungsfindung Basis/Vorschlag—ob, w s	Kriterien, Alternativen, Analysen Details: s. Anlage	
Entscheidung: Was, Wie, Wer, Wann, Mittel (Budget, Personal, sonst. Ressourcen)	Durchführung: Wie vorgeschlagen, oder abweichende Entscheidung	
Nächster/Nächste Termine	Gegenstand: Bericht, Entscheidung, Erledigung	

BJR - Nutzen

Nutzen:

- Transparente Entscheidungsgrundlagen
- Klare Entscheidungsparameter
- Einfache Kontrolle
- Schlanker Prozess bei neuen Fakten
- Haftungsvermeidung

Compliance - Begriff

- **Begriff:** Compliance – Regeltreue
- **Inhalt, Maßstab:**
  - Recht und Gesetz, Verträge
  - Standards, Practices und Konventionen
  - Betriebsvereinbarungen, Anweisungen
- **Ziel und Nutzen**
  - Risikominimierung – Rechtsverletzungen, Reputation
  - Effizienzsteigerung – klare Kriterien, schnelle Reaktion
  - Effektivitätsgewinn – Bessere Entscheidungen, Sicherheit
- **BJR in der Compliance**
  - Pflicht zu angemessener Complianceorganisation folgt aus der Leitungs- und Organisationsverantwortung
  - Fehlende Regeltreue ist unmittelbar haftungsrelevant

IT-Compliance

- Dimensionen der Compliance in der IT:
- Recht : EU-Richtlinien, internationale Konventionen, Gesetze, ggf. Handelsbräuche, vertragliche Verpflichtungen
- Ethik: Ethik-Standards der Firma, der Branche (Selbstverpflichtungen)
- Persönliche Pflichten: Arbeitsvertrag, Betriebsvereinbarungen, Handbücher, Dokumentationspflichten
- Technik: Informationssicherheit, Verfügbarkeit, Funktionsfähigkeit, Datenaufbewahrung und Datenschutz

IT-Governance

Begriff:

„Organisations-Compliance“, umfasst zusätzlich zu IT-Compliance Controlling, Prozesse, Berichtswege und Verantwortlichkeiten

Inhalt:

Schaffung eines konsistenten Organisations-Rahmens der IT-Organisation und der Schnittstellen sichert Effizienz und Effektivität

Vorteile: Vermeidung von Organisationsverschulden durch: Ordnung, Übersicht und Transparenz

- Klare Kompetenzordnung sowie Aufgaben- und Verantwortlichkeitsabgrenzung
- Klare Berichtslinien und Berichtspflichten
- Transparente Aufbau- und Ablauforganisation
- Systematische Regelungen zur Ausgestaltung der Risikosteuerungs- und der Controllingprozesse

BJR – Compliance – CG -> Fazit

- **BJR als anerkanntes Vorgehen bei der Entscheidungsfindung schafft effektiv Freiraum für produktive Arbeit**
- **Compliance - mit Augenmaß betrieben – ist ein Muss**
- **Gute Governance schützt alle Beteiligten vor Überraschungen und Haftung**

Gerne unterstütze ich Sie

Sprechen Sie mich an: Beratung, Workshops...

Quellen

§ 93 Aktiengesetz

Sorgfaltspflicht und Verantwortlichkeit der Vorstandsmitglieder

(1) Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln. …

(2) **Vorstandsmitglieder**, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet. Ist streitig, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, so **trifft** sie **die Beweislast**.

§ 43 GmbHG Haftung der Geschäftsführer

(1) Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.

(2) Geschäftsführer, welche ihre Obliegenheiten verletzen, haften der Gesellschaft solidarisch für den entstandenen Schaden.

Quellen

§ 130 OWiG

(1) Wer als Inhaber eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, handelt ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre. Zu den erforderlichen Aufsichtsmaßnahmen gehören auch die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen.

(2) …

(3) Die Ordnungswidrigkeit kann, wenn die Pflichtverletzung mit Strafe bedroht ist, mit einer Geldbuße bis zu einer Million Euro geahndet werden. Ist die Pflichtverletzung mit Geldbuße bedroht, so bestimmt sich das Höchstmaß der Geldbuße wegen der Aufsichtspflicht-verletzung nach dem für die Pflichtverletzung angedrohten Höchstmaß der Geldbuße. Satz 2 gilt auch im Falle einer Pflichtverletzung, die gleichzeitig mit Strafe und Geldbuße bedroht ist, wenn das für die Pflichtverletzung angedrohte Höchstmaß der Geldbuße das Höchstmaß nach Satz 1 übersteigt.

Quellen

SELBSTTEST NACH IDW PS 980

Diese sieben Grundelemente braucht jedes Compliance-Management-System (CMS)

Compliance-Kultur – die klare Botschaft des Managements über die für das Selbstverständnis des Unternehmens tragenden Grundwerte

Compliance-Ziele – sagen, was das CMS erreichen soll, zum Beispiel: Verhinderung von Korruption oder von Verstößen gegen Umwelt- bzw. Datenschutzbestimmungen. Die Ziele können sich auch auf Teilbereiche – bestimmte Risiken, Regionen, Geschäftsfelder – beziehen. Müssen integraler Bestandteil der Geschäftsziele und der Unternehmensstrategie sein

Compliance-Risiken – werden in systematischen Verfahren und Berichterstattung identifiziert, ihre Eintrittswahrscheinlichkeit analysiert

Compliance-Programm – nennt Grundsätze und Maßnahmen zur Begrenzung der Compliance-Risiken und zum Verhalten bei Verstößen

Compliance-Organisation – umfasst personelle und andere Ressourcen, definiert Rollen, Verantwortlichkeiten und Abläufe

Compliance-Kommunikation – umfasst die Unterrichtung der Mitarbeiter über das Compliance-Programm, ihre Rollen und Verantwortlichkeiten sowie die Einrichtung von Kommunikationswegen im Unternehmen für die Meldung von Risiken und Verstößen. Nach außen werden Verhaltensstandards gegenüber Geschäftspartnern kommuniziert, außerdem etwa eine Selbstverpflichtung gegenüber Öffentlichkeit und Medien

Überwachung und Verbesserung – ein CMS muss laufend auf Angemessenheit und Wirksamkeit geprüft, optimiert und an neue Entwicklungen angepasst sowie von Schwachstellen und Mängeln befreit werden. Das erfordert Reporting und Dokumentation