BVMed-Akademie

4. November 2026

Compliance-Organisation für MedTech-Unternehmen

Referenten:

RAin Christiane Döring, Ahrensburg

RA Prof. Dr. Hendrik Schneider, Wiesbaden

Agenda

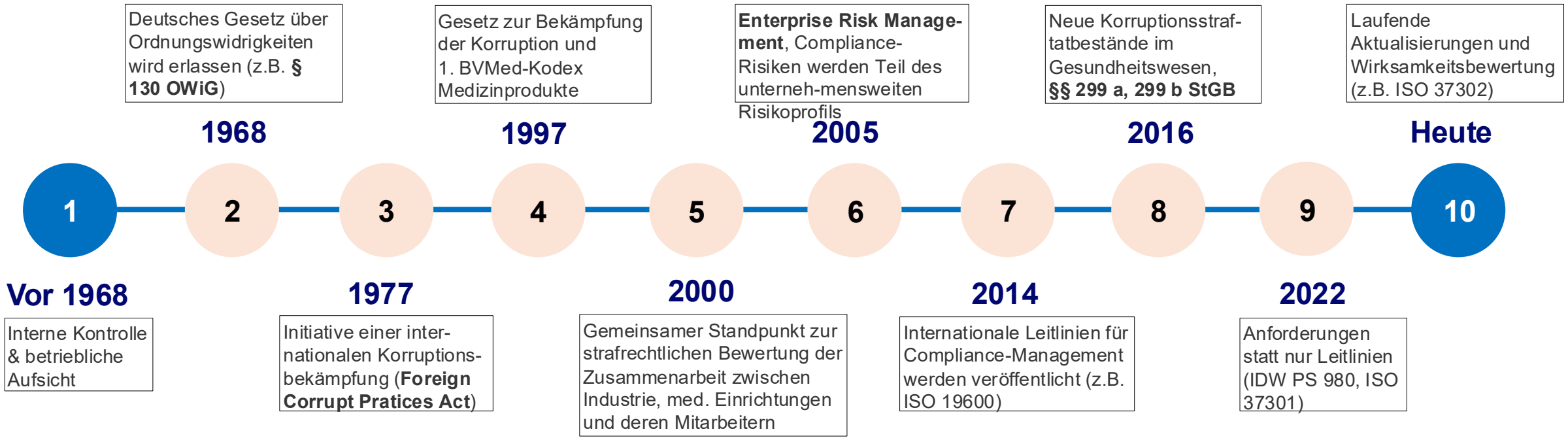
Compliance-Organisation für MedTech-Unternehmen

A. **Compliance-Risikoanalyse**
   - I. **Historische Entwicklung**
   - II. **Definition**
   - III. **Analyseziele**
   - IV. **Analyse-Werkzeug**
   - V. **Risikofelder**
   - VI. **Fälle aus der Rechtsprechungs-Praxis**
   - VII. **Fallbeispiel**

B. Hinweisgebersystem
C. Grundelemente eines Compliance-Management-Systems (CMS)
D. Compliance-Audit
E. Interne Untersuchungen und Sanktionen
F. Haftungsprävention durch Dokumentation und Schulung

A. Compliance-Risikoanalyse

I. Historische Entwicklung



Was zeigt die historische Entwicklung?

Compliance hat den Weg von der Einzelkontrolle zum Gesamtsystem beschritten. Unternehmen sollen ihre Regelkenntnis zur **Prävention von Verstößen** nutzen. Formale Richtlinien müssen durch **nachweisbare Wirksamkeit** ergänzt werden. Zwar gibt es keine allgemeine Pflicht für Unternehmen zu einem CMS in bestimmter Form, die Geschäftsführung muss aber ihre **Organisations- und Überwachungspflichten** erfüllen. Welche Maßnahmen erforderlich sind, hängt insbesondere von **Größe, Geschäftsmodell und Risikolage** ab.

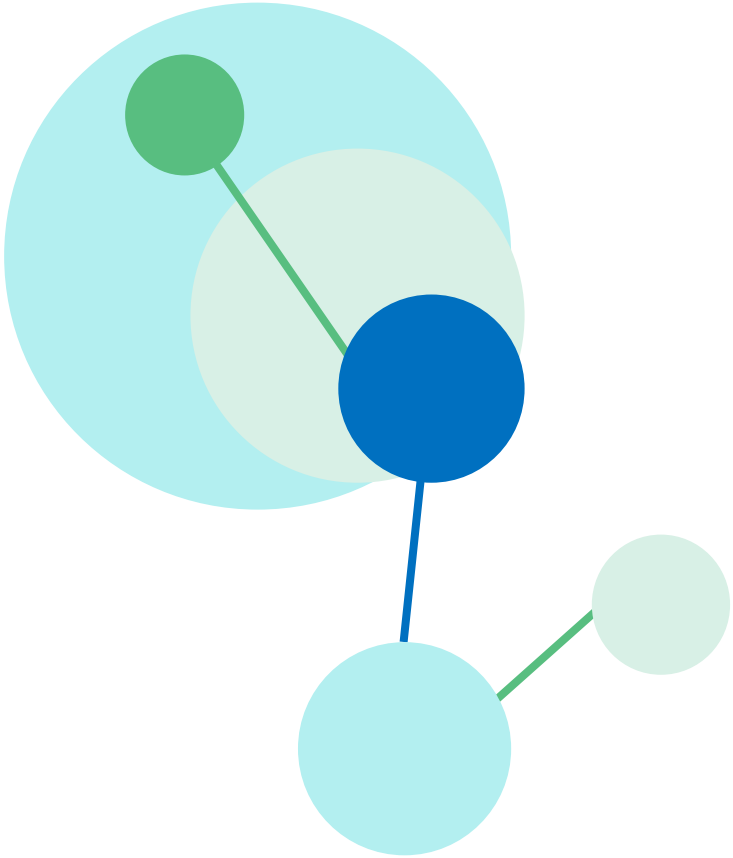
A. Compliance-Risikoanalyse

II. Definition

Die Compliance-Risikoanalyse ist ein Unternehmensprozess, in dem ermittelt, bewertet und priorisiert wird, wo und wie gegen Gesetze, regulatorische Vorschriften, interne Richtlinien oder ethische Standards verstoßen werden könnte.

- **Compliance: Einhaltung der für eine Organisation geltenden rechtlichen, regulatorischen und internen Vorgaben.**

- **Risikoanalyse: Systematische Identifikation und Bewertung möglicher Ereignisse, ihrer Eintrittswahrscheinlichkeit und ihrer Auswirkungen.**



A. Compliance-Risikoanalyse

III. Analyseziele

1. Erfassen der Compliance-Verpflichtungen

Relevante Gesetze, regulatorische Vorgaben, Verordnungen, Verträge, Genehmigungen, interne Richtlinien und sonstige verbindlichen Anforderungen kennen und einhalten.

2. Identifikation der Risiken

Geschäftsprozesse, Transaktionen und Geschäftspartner auf potenzielle Risiken überprüfen und Fehlentwicklungen vor Eintritt von Schäden entdecken.

3. Bewertung der gefundenen Risiken

Eintrittswahrscheinlichkeit und **Schadensausmaß** unter Berücksichtigung der vorhandenen Kontrollen einschätzen.

4. Priorisierung der Risiken

Identifizierte **verhaltens- und organisationsbezogene Risiken** in einem Risikoregister (Risikomatrix) zusammenführen und Maßnahmen nach dem ermittelten **Risiko-Score** gewichten.

5. Festlegen von Maßnahmen

Vorgehensweisen bei Freigabeprozessen (Vier-Augen-Prinzip), Schulungen, Geschäftspartnerprüfungen und technischen Kontrollen implementieren.

6. Überwachung & Aktualisierung der Maßnahmen

Wirksamkeit der Maßnahmen prüfen und die Analyse bei Veränderungen oder neuen Erkenntnissen aktualisieren.

Unternehmensziel: Vertrauen und Reputation schützen.

A. Compliance-Risikoanalyse

IV. Werkzeug für die Risiko-Analyse

A. Faktoren für die Eintrittswahrscheinlichkeit

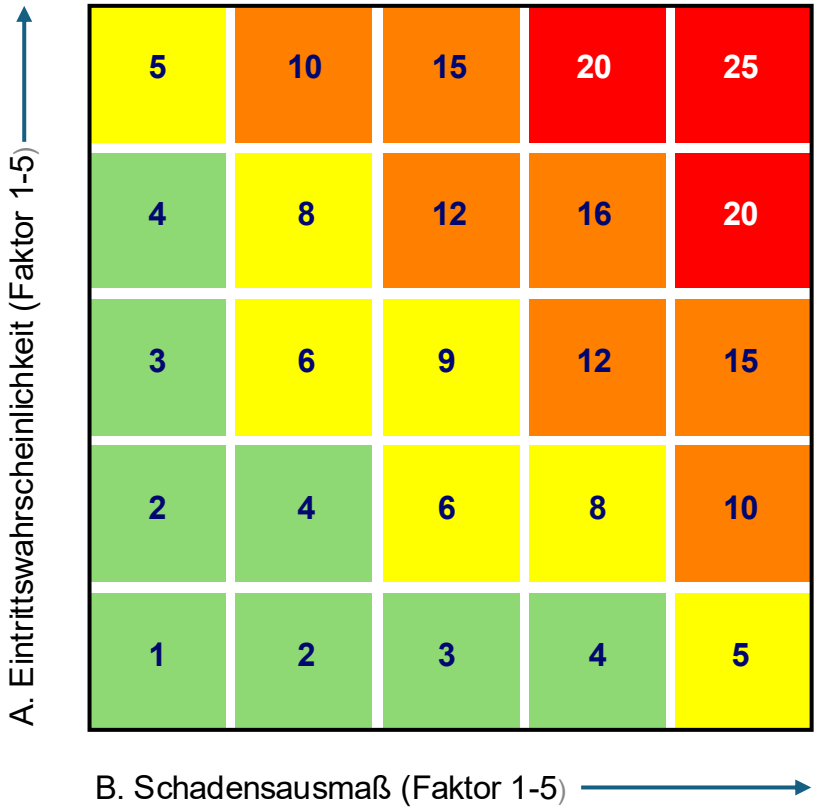
x1 = sehr unwahrscheinlich
x2 = unwahrscheinlich
x3 = möglich
x4 = wahrscheinlich
x5 = sehr wahrscheinlich

B. Faktoren für das Schadensausmaß

x1 = geringfügig
x2 = begrenzt
x3 = erheblich
x4 = schwerwiegend
x5 = besonders gravierend

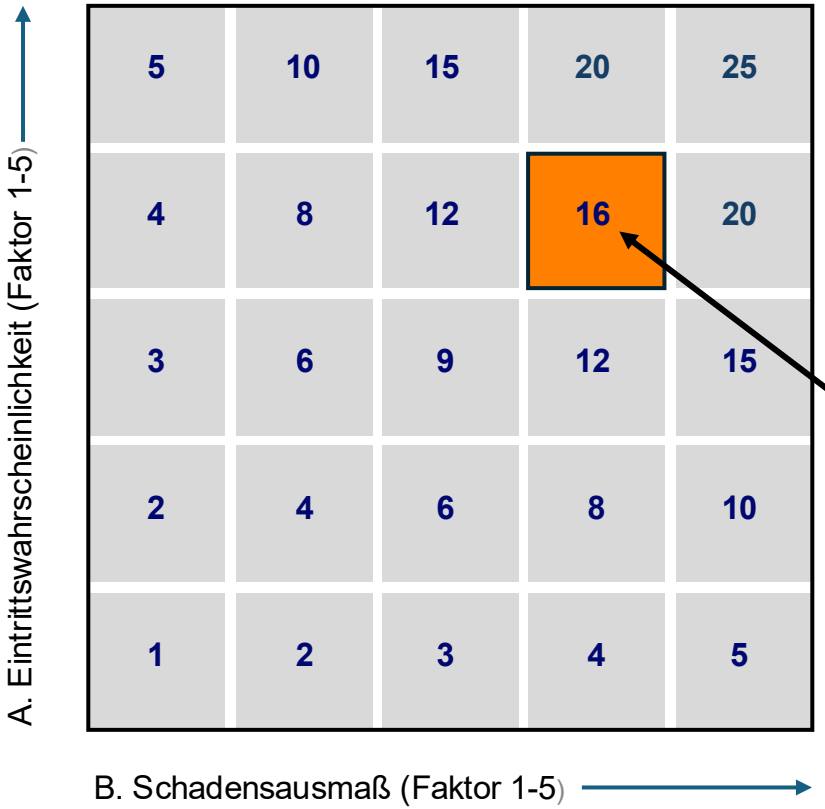
C. Ergebnis (Risiko-Score)

Eintrittswahrscheinlichkeit multipliziert mit dem Schadensausmaß



A. Compliance-Risikoanalyse

IV. Werkzeug für die Risiko-Analyse



Risiko-Interpretation

1–4 NIEDRIG

Bestehende Kontrollen regelmäßig überprüfen.

Kein unmittelbarer Handlungsdruck.

5–9 MITTEL

Verbesserung prüfen.

Verantwortlichen und angemessene Frist festlegen.

10–16 HOCH

Maßnahmen priorisieren.

Geschäftsführung bzw. Fachverantwortung einbinden.

17–25 KRITISCH

Unmittelbaren Handlungsbedarf prüfen.

Eskalation und kurzfristige Risikoreduktion.

A. Compliance-Risikoanalyse

IV. Werkzeug für die Risiko-Analyse

Erarbeitung einer intialen Risiko Matrix (Fallbeispiel Medizinprodukte)

Rot = Risiko nicht kontrolliert
Gelb = Risiko teilweise kontrolliert
Grün = Risiko kontrolliert
(keine Aussage zur tatsächliche Befolgung aller Regeln! Dies ist im Nachgang durch eine Wirksamkeitsprüfung zu überprüfen)

Compliance-/Themenbezogene Gliederung												
	Rot = hohes compliance-relevantes Risikopotential **Gelb** = mittleres compliance-relevantes Risikopotential **Grün** = geringes compliance-relevantes Risikopotential		**Gefährdetes Gut/Rechtsgut**	**Spezialgesetzliche Compliance-Vor-gaben/Kodizes**	**Ergriffene Compliance Maßnahmen (Richtlinien, Prozesse, Schulungsmaßnahmen etc.)**	**Einhaltung/Überwachung (wer, wann, wie?)**	**Analyse: sind die ergriffenen Compliance-Maßnahmen**			**Wird dem Risiko durch geeignete Maßnahmen begegnet? (Grad der Risikokontrolle)**	**Zu ergreifende weitere Compliance Maßnahmen**
Themen	**Unterthemen I**	**Unterthemen II**					**geeignet?**	**wirksam implementiert?**	**vollständig?**		
Corporate	Compliance Management System	Grundwerte, Code of Conduct									
		Horizontale und vertikale Delegation sowie Abgrenzung der Compliance-Verantwortlichkeiten	Vermögen/persönliche Haftung der Organe	§§ 130, 30 OWiG							
		Verbindliche Compliance-Organisationsrichlinie/-Verfassung									
		Systematische Erfassung und Bewältigung Compliance-relevanter Risiken durch continuous Risk-Assessment									
		Tone from the Top									

Beispielsmatrix des BVMed: https://www.bvmed.de/themen/compliance

- Start durch Anwendung auf die eigenen **Unternehmens-Spezifikationen**.
- Fokus: **Schadenshöhe** und **Schadenseintrittswahrscheinlichkeit**. **Strafrechtsrelevanz**.
- Es entsteht eine „Risiko-Landkarte“, die jederzeitige Orientierung über die Risiken des Unternehmens in den jeweiligen Fachabteilungen und in der jeweiligen Branche, hier: Gesundheitsmarkt, gibt.

A. Compliance-Risikoanalyse

V. Risikofelder

Risikofeld	Typische Konstellationen / Kooperationen in der Medizinproduktebranche	Zentrale Rechtsgüter
Korruption im Gesundheitswesen	Kooperationen mit Ärzten/HCP, Kliniken und sonstigen Leistungserbringern; Berater-/Referentenverträge; Vergütungen, Sachleistungen oder sonstige Vorteile für Verordnung, Bezug oder Zuführung von Patienten	Unabhängigkeit heilberuflicher Entscheidungen; Lauterkeit des Wettbewerbs, §§ 299a/b StGB
Zuweisung / Verordnungssteuerung	Patienten-, Rezept- oder Verordnungszuführung; Einflussnahme auf die Wahl des Leistungserbringers oder Produkts; Kopplung von Vorteilen an Verordnungen oder Versorgungen; Homecare-Rezeptmanagement	Freie und unbeeinflusste Therapie-, Verordnungs- und Versorgungsentscheidung; Patientenautonomie; fairer Wettbewerb, §§ 128, 73 Abs. 7 SGB V, 31 MBO-Ä
Unzulässige Zuwendungen	Geschenke, Bewirtung, Reisekosten, kostenlose Produkte/Leistungen, Schulungen oder sonstige Vorteile für HCP, Kliniken, Apotheken oder Leistungserbringer	Unabhängigkeit der Entscheidungsträger; Schutz vor unsachlicher Einflussnahme; Lauterkeit des Wettbewerbs
Abrechnungsbetrug / Abrechnungsmanipulation	Falsch-/Fehlabrechnung; nicht erbrachte Leistungen, unzutreffende Dokumentation; Einflussnahme auf Rezept- und Versorgungsdokumentation; sonstige unzulässige Abrechnungskonstellationen	Vermögen der Kostenträger; Integrität und Funktionsfähigkeit des Gesundheits- und Abrechnungssystems; Nullretaxation; Vermögensabschöpfung, § 263 StGB
Unzulässige Leistungserbringer-Kooperationen	Zuweisungs-, Beteiligungs- oder Vergütungsmodelle; unzulässige Zusammenarbeit zwischen Ärzten, Apotheken, Homecare-/Hilfsmittelleistungserbringern und Herstellern; wirtschaftliche Verknüpfung von Versorgung und Vorteil	Patienten-/Versorgungsinteressen; freie Leistungserbringerwahl; Wettbewerb; Wirtschaftlichkeit der GKV

A. Compliance-Risikoanalyse

V. Risikofelder

Risikofeld	Typische Konstellationen / Kooperationen in der Medizinproduktebranche	Zentrale Rechtsgüter
Apothekenbezogene Kooperationen	Bevorzugte Belieferung, Zuführung von Patienten oder Verordnungen, wirtschaftliche Vorteile im Zusammenhang mit der Arzneimittelversorgung	Unabhängigkeit der Arzneimittelversorgung; freie Wahl des Apothekers; Lauterkeit des Wettbewerbs, § 11 ApoG
Unzulässige Heilmittelwerbung / Produktbeeinflussung	Unzulässige Zuwendungen oder Werbegaben; irreführende oder unsachliche Produktwerbung; Einflussnahme auf HCP oder Verbraucher	Gesundheitsschutz; Schutz vor unsachlicher Beeinflussung; Lauterkeit des Wettbewerbs, § 7 ff. HWG
Datenschutz und IT-Sicherheit	Unberechtigter Datenzugriff auf Gesundheitsdaten (intern & extern) und/oder Fehlversand sensibler Informationen	Patientenrechte und –wahlmöglichkeiten nach SGB, DSGVO und BDSG

Rechtsgrundlagen: §§ 299a, 299b, 263 StGB; §§ 73 Abs. 7, 128 SGB V; § 11 ApoG; § 7 ff. HWG; § 31 MBO-Ä; UWG.

⇨ **Besonders schadensträchtig sind Risiko-Konstellationen, in denen wirtschaftliche Vorteile, Verordnung, Zuweisung, Versorgung und Abrechnung miteinander verknüpft werden. Das Risiko entsteht aus der konkreten Kooperations-Beziehung.**

A. Compliance-Risikoanalyse

VI. Fälle aus der Rechtsprechungs-Praxis

Fall-Konstellation	Gericht	Compliance-Hinweis
Payback-Punkte für Hörgeräte	**BGH v. 17.07.2025 – I ZR 43/24**	Überschreitung der Geringwertigkeitsgrenze aus § 7 HWG; 1 Euro-Schwelle auch für Medizinprodukte
„Luftrezepte“ für Sprechstundenbedarf	**LG Leipzig v. 24.06.2025, Az. 15 KLs 601 Js 72578117**	Verstoß gegen § 11 ApoG (Zuweisungsverbot) Betrug nach § 263 StGB ggü der Krankenkasse durch Abrechnung von Rezepten für nicht abgegebene Arzneimittel
Sanitätshaus-Provision an Ärztin	**BGH v. 21.03.2024 – 3 StR 163/33**	Vorteilsgewährung für Patientenzuweisung, Korruption gemäß §§ 299a/b StGB; Freiheitsstrafe 2 Jahre 6 Monate + Wertersatz
Kooperation mit einer “Vorzugs“- Apotheke	**LSG Niedersachsen-Bremen v. 10.03.2024, L 4 KR 260/22; vgl. BGH v. 18.06.2015 – I ZR 26/14**	Verstoß gegen § 11 ApoG (Zuweisungsverbot); keine Vergütung für Zuweisungen oder Verordnungen; Retaxierung auf Null
Überhöhtes Chefarztgehalt	**LAG SH v. 05.03.2024, 2 Sa 125 öD/23**	Keine Indizien für Verstoß gegen §§ 299a/b StGB, hohe Vergütung allein reicht nicht
Teure Geschenke	**BGH v. 09.09.2010 – I ZR 193/07**	Teure Geschenke ohne fachlichen Bezug - Gegenleistung für Verordnungen
Überhöhte Vortragshonorare an Ärzte	**LG Hamburg v. 9.10.2010, 618 KLs 10/09**	Überhöhte Vertragshonorare - Gegenleistung für Verordnungen

Fallbeispiel 1: Compliance-Risikoanalyse

Fall 1: „Das neue Versorgungsmodell“

Medizinproduktehersteller M ist ein mittelständisches Unternehmen mit ca. 380 Mitarbeitern und vertreibt Geräte für die Kaltplasmatherapie, eine spezielle Form der Wundversorgung. M ist in den letzten Jahren stark gewachsen. Es gibt einen Compliance-Officer, der organisatorisch dem CFO zugeordnet ist.

Der Vertrieb schlägt der Geschäftsführung ein neues Versorgungsmodell vor:

Ein großer MVZ-Verbund soll als Pilotkunde gewonnen werden.

Ein leitender Arzt des MVZ-Verbundes soll das Unternehmen bei der Entwicklung des neuen Versorgungsmodells beraten. Dafür soll er einen **Beratervertrag** über 30.000 € jährlich erhalten.

Zusätzlich soll das MVZ **kostenfrei Produkte** und technische Unterstützung erhalten.

Der Vertrieb möchte dem MVZ-Verbund einen „**besonders attraktiven Einführungspreis**“ anbieten.

Ein externer Vertriebspartner erhält eine **erfolgsabhängige Vergütung**, wenn der MVZ-Verbund das Produkt in mehreren Häusern einsetzt.

Die Geschäftsführung fragt den Compliance-Officer: ***„Können wir das so machen?“***

Der Compliance-Officer hört zum ersten Mal von dem Projekt und kennt die einzelnen Vorgänge nicht.

Welche Informationen brauchen Sie als Compliance-Officer, um die Compliance-Risiken des Projektes zu bewerten?

Fallbeispiel 1 zum Einstieg in die Compliance-Risikoanalyse

Fallbeispiel 1: „Das neue Versorgungsmodell“

Informationsbedarf zur Risikobewertung:

1. Wer steht rechtlich hinter dem MVZ-Verbund, insbesondere öffentlich-rechtliche Trägerschaft, rechtlich selbständige Einheiten, ambulant oder stationär?
2. Welche Rolle hat der beratende Arzt in dem MVZ-Verbund?
3. Was genau soll der Arzt beraten und welche Leistungen soll er erbringen? Wonach wurde gerade dieser Arzt ausgewählt?
4. Wofür sollen die kostenfrei bereitgestellten Produkte und Leistungen eingesetzt werden?
5. Wie wurde der besonders attraktive Einführungspreis kalkuliert?
6. Wovon hängt die Vergütung für den Vertriebspartner konkret ab?
7. Wer entscheidet auf Seiten des MVZ-Verbundes über die Einführung und Beschaffung?
8. Gibt es interne Vorgaben für solche Projekte?
9. Warum erfährt der Compliance-Officer erst jetzt von dem Projekt?

⇨ **Wir haben gerade eine kleine Compliance-Risiko-Analyse durchgeführt.**

Vor der Kaffeepause geht es erst noch weiter...



… mit dem Hinweisgebersystem

Haftungsausschluss und Copyright:

Alle Informationen, die in dieser Präsentation enthalten sind, erheben keinen Anspruch auf Vollständigkeit.

Es wird keine ausdrückliche oder stillschweigende Zusicherung oder Gewährleistung für die Richtigkeit oder Vollständigkeit der in dieser Präsentation enthaltenen Informationen gegeben.

Alle Inhalte dieser Präsentation sind urheberrechtlich geschützt.

© RAin Christiane Döring, © RA Prof. Dr. Hendrik Schneider

Kontakt



Rechtsanwältin Christiane Döring

Hagener Allee 50
22926 Ahrensburg
Tel.: +49 173 2010175
c.doering@doering-rechtsanwalt.de



Prof. Dr. jur. Hendrik Schneider

Taunusstraße 5a
65183 Wiesbaden
Tel + 49 (0) 611 950 08110
schneider@hendrikschneider.eu
www.hendrikschneider.eu