BVMED
HEALTHCARE COMPLIANCE SCHULUNG
UMSETZUNG DES
COMPLIANCE-MANAGMENT-SYSTEMS

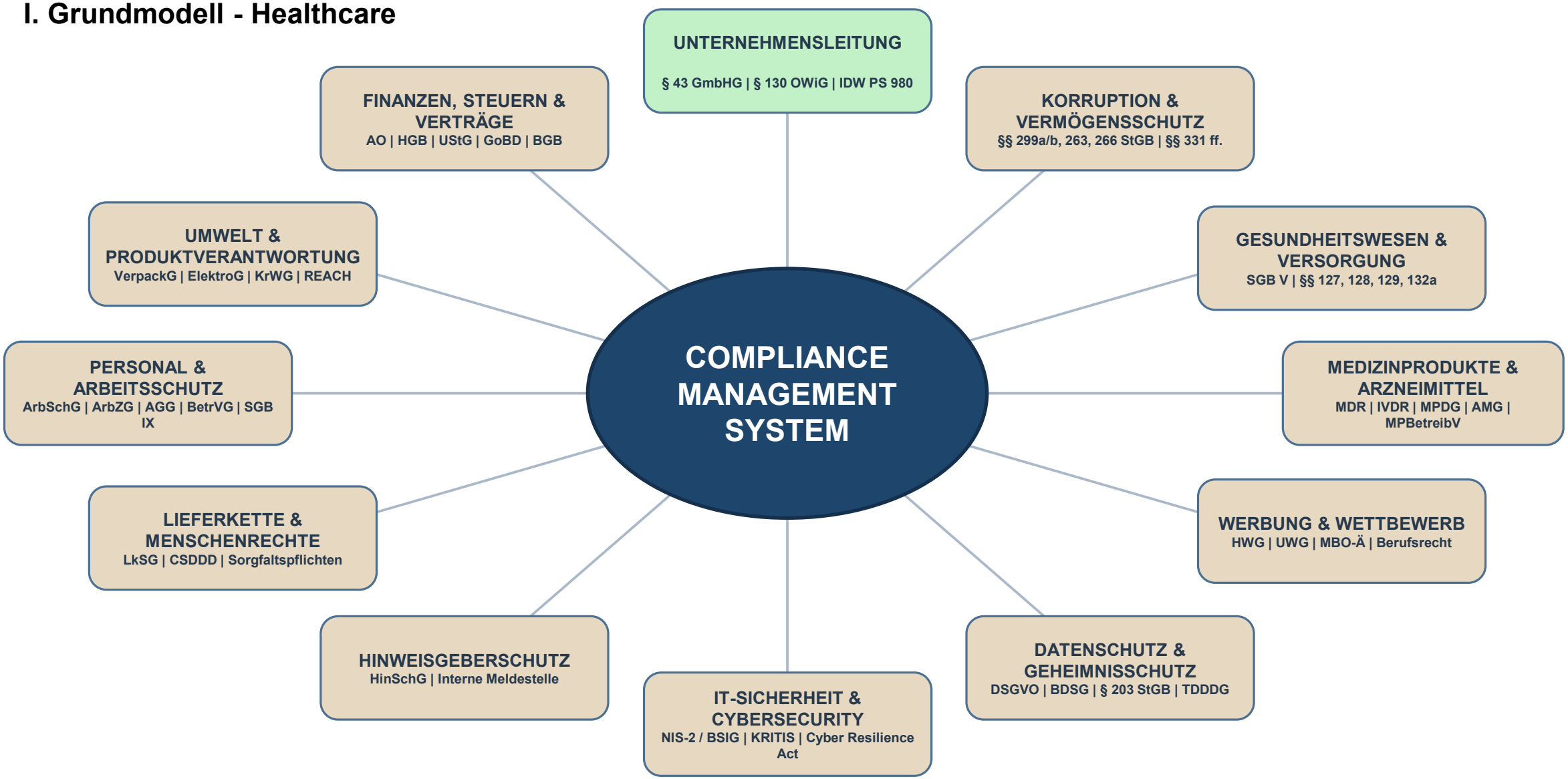
Rechtsanwältin Christiane Döring
am 17. November 2026

AGENDA

Compliance-Management-System (CMS)

I. Grundmodell - Healthcare
II. Einstiegsfall
III. Rechtsgrundlagen
IV. Installation eines kompletten CMS
V. Fälle aus der Rechtsprechungs-Praxis
VI. Zurück zum Einstiegsfall

I. Grundmodell - Healthcare



II. Einstiegsfall in das Compliance-Management-System

„Wer Risiken kennt, muss handeln“

Die **MedTech GmbH** vertreibt seit Jahren erfolgreich Augenlaser-Systeme.

Compliance-Themen werden zwar gelegentlich diskutiert, ein strukturiertes **Compliance-Management-System** existiert aber nicht: Verbindliche Regeln für Einladungen und Bewirtungen von Ärzten fehlen ebenso wie regelmäßige Schulungen, klare Zuständigkeiten oder wirksame Kontrollen.

Der Vertriebsmitarbeiter Vorschnell überschreitet wiederholt die Grenzen des Zulässigen. Über Jahre werden Ärzte mit Einladungen, Bewirtungen und sonstigen Vorteilen bedacht. Das Vorgehen von Herrn Vorschnell wird schließlich den Gesellschaftern bekannt.

Die Folgen sind erheblich: Interne Untersuchungen, Anwaltskosten, behördliche Ermittlungen, Reputationsschäden und wirtschaftliche Einbußen.

Die MedTech GmbH prüft, ob sie ihren Geschäftsführer persönlich auf Schadenersatz in Anspruch nehmen kann.

Der Geschäftsführer verteidigt sich:

„Von den einzelnen Vorgängen wusste ich nichts. Dafür waren doch meine Mitarbeiter verantwortlich!“

Hat der Geschäftsführer damit bereits das entscheidende Argument auf seiner Seite oder was hätte er organisatorisch sicherstellen müssen?

III. Rechtsgrundlagen

Braucht Ihr Unternehmen ein Compliance-Management-System?

- **Keine allgemeine gesetzliche Pflicht zur Errichtung eines Compliance Management Systems:** Das deutsche Recht (z.B. GmbHG) kennt keine explizite Vorschrift, die ein Unternehmen zur Errichtung eines CMS zwingt (*Lösler*, in: Mosmayer/Lösler (Hrsg.), Corporate Compliance, § 1 Rn. 29.)
- **Aber:** Die Geschäftsführung muss die gesetzlichen Anforderungen an eine ordnungsgemäße Unternehmensorganisation erfüllen. Welche Maßnahmen erforderlich sind, richtet sich insbesondere nach Geschäftsmodell, Größe, Risikoprofil und konkreten Gefährdungslagen. Ableitung:
  - **§ 43 Abs. 1 GmbHG**: Pflicht zur Sorgfalt eines ordentlichen Kaufmannes; daraus folgen Organisations- und Überwachungspflichten, insbesondere bei regulierten Medizinprodukten.
  - **§ 130 OWiG**: Erforderliche Aufsichtsmaßnahmen müssen getroffen werden, um betriebsbezogene Pflichtverletzungen zu verhindern oder wesentlich zu erschweren.
  - **§ 1 StaRUG** (Krisenfrüherkennung): seit 2021 Verpflichtung zur fortlaufenden Überwachung von Entwicklungen, die den Fortbestand des Unternehmens gefährden können, und zum Ergreifen geeigneter Gegenmaßnahmen.

Was sagt die Rechtsprechung dazu?

- **Pflicht zur Organisation und Überwachung:** Eine Delegation der Aufgabe entlastet die Unternehmensleitung nicht vollständig, so LG München I, Urteil v. 10.12.2013 – 5 HK O 1387/10 (Siemens-Fall).
- **Persönliche Haftung des Geschäftsführers:** Unzureichende Organisations- und Kontrollstrukturen können zur Geschäftsführer-Haftung führen, insbesondere wenn die Kontrolle bei schadensträchtigen Tätigkeiten fehlt, OLG Nürnberg, Urteil v. 30.03.2022 – 12 U 1520/19.

III. Rechtsgrundlagen

Ein CMS schützt nicht vor jedem Vorwurf, kann aber entlasten.

- Die Verantwortung für eine angemessene Organisation, Auswahl und Überwachung bleibt bei der Geschäftsführung.

Was sagt die Rechtsprechung hierzu?

- **Berücksichtigung bei der Unternehmensgeldbuße:** Ein wirksames CMS kann die Geldbuße bei Rechtsverstößen reduzieren, BGH v. 9.05.2017 – 1 StR 265/16.
- Dies gilt auch dann, wenn umfassende Compliance-Maßnahmen erst nach dem Verstoß eingeführt worden sind, BGH v. 27.04.2022 – 5 StR 278/21.

Was bedeutet das für die Geschäftsführung?

Ein angemessenes, dokumentiertes und gelebtes CMS hilft, Risiken frühzeitig zu erkennen, Verstöße zu verhindern und die Erfüllung der **Organisations- und Überwachungspflichten** nachvollziehbar zu belegen.

Zur Haftungsvermeidung sollte das CMS die Voraussetzungen der einschlägigen Prüfstandards erfüllen, **IDW PS 980** und mit Blick auf Ressourcen und Personal hinreichend ausgestattet sein.

Praxis-Tipp: Eine verantwortungsbewusste Geschäftsführung schafft Compliance-Strukturen, die zum **Geschäftsmodell**, zur **Unternehmensgröße** und zum **individuellen Risikoprofil** passen, maßgeschneidert statt von der Stange. Dafür dient das **individuelle Compliance-Management-System**.

IV. Installation eines kompletten CMS - Schritt 1: Verhaltenskodex

„TONE FROM THE TOP“ UND ZIELSTELLUNG :

Die Geschäftsführung dokumentiert im **Verhaltenskodex** ihr Werteverständnis für ethisches und integres Verhalten und setzt damit die Leitplanken für eine **Compliance-Kultur** im Unternehmen. „*Der Verhaltenskodex formuliert die maßgeblichen Leitlinien für unser Verhalten gegenüber unseren Kunden, Mitarbeitern, Lieferanten, Geschäftspartnern und anderen Stakeholdern“.*

Konkrete Compliance-Regelungen: Richtlinien, Leitfäden und Vorgaben, Start: für die im Rahmen der Risikoanalyse identifizierten risikobehafteten Geschäftsvorgänge:

- Kooperationen, insbesondere Umgang mit HCP und Vertriebspartnern, Vermeidung von Interessenkonflikten
- Umgang mit Zuwendungen, Einladungen, Bewirtungen, Geschenken, insbesondere bei HCP
- Datenschutz und Cybersicherheit
- Gesundheitsschutz und Sicherheit.
- Faire Arbeitsbedingungen und Menschenrechte. Diversität und Inklusion.
- Nachhaltigkeit und Umweltschutz.

IV. Installation eines kompletten CMS - Schritt 2: Compliance-Risikoanalyse

VERANTWORTUNG: Die **Geschäftsführung** mit Unterstützung: Compliance, Legal bzw. externe Rechtsberatung.

VORGEHEN: Bestandsaufnahme des Status Quo nach: Geschäftsbereich, Schadenseintrittswahrscheinlichkeit, Schadenshöhe, Strafrechtsrelevanz, bestehende Kontroll-/ Compliance-Strukturen.

ZIEL: Maßnahmen identifizieren, priorisieren und umsetzen sowie deren Wirksamkeit fortlaufend überprüfen. Ressourcen dort einsetzen, wo die Risiken am größten sind. **Compliance folgt dem Risiko!**

TOP 1: Sales & Marketing/ Medical Affairs: aktiv – umsatzgetrieben – ext. Repräsentanz ⇨ Korruption, Zuwendung

Kongresse & Sponsoring, Ärzte/ HCP/ KOL-Kooperationen, Produktdemonstrationen, Leihstellungen von Geräten,…

TOP 2: Einkauf & Lieferanten: aktiv/ passiv – umsatzgetrieben – externe Partner ⇨ Korruption, Interessenkonflikte

Lieferanten-Verträge, Rabatt- und Bonussystem, Kick-backs, Sachzuwendungen, Auswahl und Überwachung von Partnern

TOP 3: Datenschutz & Cyber-Security („IT“?): unternehmensweit – hohe Schadensdynamik ⇨ Datensicherheit

Patientendaten, Vernetzte Medizinprodukte, Fernwartung, Cybervorfälle und Reaktions- und Eskalationsprozesse

IV. Installation eines kompletten CMS - Schritt 3: Hinweisgebersystem

VERANTWORTUNG: Die **Geschäftsführung** mit Unterstützung: Compliance, Legal bzw. externe Rechtsberatung.

ZIEL: Hinweise auf mögliche Compliance-Verstöße **frühzeitig erkennen, prüfen und angemessen bearbeiten** – mit einem geschützten und vertrauenswürdigen Meldeweg. Die Umsetzung ist seit Dezember 2023 **gesetzlich verpflichtend** für Unternehmen mit mindestens 50 Mitarbeitenden. **Kernelemente:**

- **Niederschwelliger Zugang:** interne und externe Meldewege; einfache Erreichbarkeit, ggf. über die Website.
- **Vertraulichkeit & Schutz:** Identität der hinweisgebenden Person schützen; Benachteiligungen verhindern.
- **Klare Kommunikation:** Was kann gemeldet werden? An wen? Wie läuft die Bearbeitung? **Compliance-Meldung ≠ allgemeine Beschwerde.**
- **Dokumentation & Datenschutz:** Dokumentation der Meldung und Bearbeitung, Rückmeldung innerhalb der gesetzlichen Vorgaben, Lösch- und Datenschutzkonzept.
- **Eskalation:** Informations- und Entscheidungswege bis zur Geschäftsführung bzw. den zuständigen Organen.

Praxis-Tipp: Mitarbeitende und Externe müssen wissen, dass ein Hinweisgebersystem existiert, wie es erreichbar ist und wofür es genutzt wird.

IV. Installation eines kompletten CMS - Schritt 4: Regelwerk & Prozesse

VERANTWORTUNG: Die **Geschäftsführung** mit Unterstützung: Compliance, Legal bzw. externe Rechtsberatung.

ZIEL: Die identifizierten Compliance-Risiken durch **klare, risikoadäquate und praxistaugliche Regeln und Prozesse** beherrschen.

1. **Bestandsaufnahme:** Was ist vorhanden und was fehlt? Verhaltenskodex & themenspezifische Richtlinien, Leitfäden und Arbeitsanweisungen; Freigabe-, Genehmigungs- und Eskalationsprozesse; Musterverträge und Compliance-Klauseln, Dokumentations- und Kontrollvorgaben.

2. **Qualitätscheck:** Sind die Regelungen tatsächlich geeignet? Wesentliche Risiken der Risikoanalyse sind erfasst; Zuständigkeiten und Entscheidungsbefugnisse sind definiert; Vorgaben sind verständlich und praxistauglich.

3. **MedTech-spezifische Risikothemen exemplarisch:** HCP-/ Ärztekooperationen und KOL-Management; Geräteüberlassung, Muster-/Teststellungen und Systembindung; Sponsoring, Fortbildung und Zuwendungen; Vertriebs- und Geschäftsmodelle/ erfolgsabhängige Vergütung; Datenschutz, Cybersecurity und vernetzte Medizinprodukte; ggf. NIS2 und sonstige regulatorische Anforderungen.

Praxis-Tipp: Nicht möglichst viele Regeln schaffen – sondern die richtigen! Ein gutes Regelwerk beantwortet für die Mitarbeiter konkret: Was darf ich? Was muss ich? Wann muss ich fragen oder eskalieren?

IV. Installation eines kompletten CMS - Schritt 5: Schulung

VERANTWORTUNG: Die **Geschäftsführung** mit Unterstützung: Compliance, Legal bzw. externe Rechtsberatung.

ZIEL: Mitarbeiter und Führungskräfte kennen die für ihre Tätigkeit relevanten Compliance-Anforderungen und wissen, **wie sie sich im konkreten Fall verhalten sollen.**

ADRESSAT: risikobasiert

- **Führungsverantwortliche:** besondere Verantwortung für Umsetzung und Vorbildfunktion
- **Risikorelevante Funktionen:** insbesondere Sales&Marketing, Einkauf, Medical Affairs
- **Übrige Mitarbeiter:** entsprechend ihrer Tätigkeit und Bezug zu Risikothemen
- **Neue Mitarbeiter:** frühzeitige Einweisung in die wesentlichen Compliance-Regeln

SCHULUNGSMETHODIK: nicht jede Zielgruppe braucht dieselbe Schulung. Je nach Risiko-Bezug: in Präsenz mit Praxisfällen und Diskussion, E-Learning für standardisierte Inhalte, mit Wissenstests. Anlass-Schulungen bei wesentlichen Änderungen oder Verstößen. Dokumentation zu Teilnahme und Schulungsstand.

Praxis-Tipp: Risikobasierte Schulung statt Gießkanne – die Mitarbeiter mit den höchsten Compliance-Risiken brauchen eine intensive und praxisnahe Schulung.

IV. Installation eines kompletten CMS - Schritt 6: Mitbestimmung

VERANTWORTUNG: Die **Geschäftsführung** mit Unterstützung: Compliance, Legal bzw. externe Rechtsberatung: frühzeitige Einbindung der Arbeitnehmervertretung soweit Mitbestimmungsrechte bestehen.

ZIEL: Compliance-Regelungen **rechtssicher, akzeptiert und wirksam** im Unternehmen verankern.

Wo kann Mitbestimmung relevant sein?

- **Compliance-Richtlinien:** sind Regelungen des betrieblichen Ordnungsverhaltens, § 87 Abs. 1 Nr. 1 BetrVG.
- **Kontroll- und Überwachungssysteme:** insbesondere bei technischen Einrichtungen, die geeignet sind, Verhalten oder Leistung der Arbeitnehmer zu überwachen, § 87 Abs. 1 Nr. 6 BetrVG.
- **Schulungen und betriebliche Maßnahmen:** Mitbestimmungsrechte sind zu beachten, insbesondere bei Fragen der betrieblichen Ordnung oder Berufsbildung.

Was bedeutet das für unser CMS?

- Frühzeitige Prüfung, ob eine Maßnahme **mitbestimmungspflichtig** ist. Rechtzeitige Einbindung der Arbeitnehmervertretung. Einführung, Kommunikation und Umsetzung abstimmen.

Praxis-Tipp: Compliance zusammen mit der Arbeitnehmervertretung organisieren. Frühzeitig prüfen, beteiligen und dann implementieren.

IV. Installation eines kompletten CMS - Schritt 7: Verstöße

VERANTWORTUNG: Die **Geschäftsführung** mit Unterstützung: Compliance, Legal bzw. externe Rechtsberatung.

ZIEL: Auf erkannte Verstöße angemessen reagieren, Wiederholungen verhindern und Schwachstellen im CMS beseitigen.

Interne Untersuchung und Sanktionen
- Interne Untersuchung zur Aufklärung
- Konsequente Reaktion auf bestätigte Verstöße, Sanktionen
- Einheitliche Maßstäbe unabhängig von Hierarchie und Funktion
- Ggf. arbeitsrechtliche Konsequenzen

Abhilfemaßnahmen
- Organisatorische Schwachstellen beseitigen
- Regelwerk bei Bedarf anpassen
- Schulungsmaßnahmen

Praxis-Tipp: Ein Verstoß ist abgeschlossen, wenn das Unternehmen die Ursache aufgeklärt und erforderliche Konsequenzen gezogen hat.

V. Fälle aus der Rechtsprechungs-Praxis

Fall-Konstellation	Gericht	Compliance-Hinweis
Arzt mit Unterschriftenstempel	**BSG v. 27.08.2025 – B 6 KA 9/24**	Formale sozialrechtliche Abrechnungsvorgaben wurden nicht eingehalten; Null-Regress.
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

VI. Zurück zum Einstiegsfall „Wer Risiken kennt, muss handeln“

Die **MedTech GmbH** vertreibt seit Jahren erfolgreich Augenlaser-Systeme.

Compliance-Themen werden zwar gelegentlich diskutiert, ein strukturiertes **Compliance-Management-System** existiert aber nicht: Verbindliche Regeln für Einladungen und Bewirtungen von Ärzten fehlen ebenso wie regelmäßige Schulungen, klare Zuständigkeiten oder wirksame Kontrollen.

Der Vertriebsmitarbeiter Vorschnell überschreitet wiederholt die Grenzen des Zulässigen. Über Jahre werden Ärzte mit Einladungen, Bewirtungen und sonstigen Vorteilen bedacht. Das Vorgehen von Herrn Vorschnell wird schließlich den Gesellschaftern bekannt.

Die Folgen sind erheblich: Interne Untersuchungen, Anwaltskosten, behördliche Ermittlungen, Reputationsschäden und wirtschaftliche Einbußen.

Die MedTech GmbH prüft, ob sie ihren Geschäftsführer persönlich auf Schadenersatz in Anspruch nehmen kann.

Der Geschäftsführer verteidigt sich:

„Von den einzelnen Vorgängen wusste ich nichts. Dafür waren doch meine Mitarbeiter verantwortlich!“

Hat der Geschäftsführer damit bereits das entscheidende Argument auf seiner Seite oder was hätte er organisatorisch sicherstellen müssen?

VI. Zurück zum Einstiegsfall: „Wer Risiken kennt, muss handeln“

Was hätte die Geschäftsführung sicherstellen müssen?

Nicht jeder Verstoß ist vermeidbar – aber erkennbare Risiken müssen angemessen gesteuert werden.

- **Vorgeben:** Verbindliche Regeln für Einladungen, Bewirtungen und sonstige Zuwendungen an Ärzte.
- **Organisieren:** Klare Zuständigkeiten, Genehmigungs- und Eskalationswege.
- **Befähigen:** Risikoorientierte Schulungen für Vertrieb und Führungskräfte.
- **Kontrollieren:** Angemessene Kontrollen und regelmäßige Überprüfung der Umsetzung.
- **Aufdecken und reagieren:** Hinweise ernst nehmen, Verdachtsfälle aufklären und erkannte Schwachstellen beseitigen.
- **Nachhalten:** Prüfen, ob die Maßnahmen wirken, und das System bei Bedarf anpassen.

Fazit für die Geschäftsführung:
Die Verantwortung für eine angemessene Compliance-Organisation bleibt bei der Geschäftsführung – auch wenn operative Aufgaben delegiert werden.

Fall in Anlehnung an OLG Nürnberg, Urteil v. 30.03.2022 – 12 U 1520/19. Im Tankkartenfall ermöglicht ein Mitarbeiter durch Manipulation in der Abrechnung erhebliche Forderungsausfälle. Der Geschäftsführer hatte keine hinreichenden Compliance-Vorkehrungen getroffen und musste rund 860.000 EUR Schadenersatz leisten.

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



KONTAKT

RECHTSANWÄLTIN
CHRISTIANE DÖRING

Hagener Allee 50, 22926 Ahrensburg
Tel. +49 (0) 173 201 0175
c.doering@doering-rechtsanwalt.de

© Kanzlei Döring