IT-Security, Risk Management & Produkthaftung

Rechtliche Einordnung | Neue Haftungsrisiken für Unternehmen und deren Entscheidungsträger

---

BVMed-Webinarreihe: Risiko Medizinprodukt
Modul 2 – 28. April 2025

Dr. iur. Dr. med. Adem Koyuncu

Rechtsanwalt und Arzt

COVINGTON

BEIJING BRUSSELS DUBAI FRANKFURT JOHANNESBURG LONDON LOS ANGELES

NEW YORK SAN FRANCISCO SEOUL SHANGHAI SILICON VALLEY WASHINGTON

www.cov.com

Ihr Referent

Dr. iur. Dr. med. Adem Koyuncu

Rechtsanwalt und Arzt

Dr. Koyuncu ist Rechtsanwalt und Arzt und Partner der Kanzlei Covington & Burling in Frankfurt. Er ist einer der Leiter der „Food, Drug & Device“-Gruppe der Kanzlei. Vor seiner anwaltlichen Tätigkeit war er in der Pharmaindustrie und als Arzt an einer deutschen Universitätsklinik tätig.

Als Anwalt ist Dr. Koyuncu einer der "führenden Berater für Pharma- und Medizinprodukterecht" in Deutschland (JUVE & Legal 500, 2024). Er berät Unternehmen u.a. zu regulatorischen Fragen sowie in den Bereichen Compliance, Datenschutz- und Haftungsrecht. Er hat vielfach Unternehmen und Manager in Haftungsfragen beraten und vor Gericht und in anderen Verfahren verteidigt.

Dr. Koyuncu ist seit vielen Jahren Mitglied im Arbeitskreis Recht (AKR) des BVMed. Er ist auch Lehrbeauftragter an den Universitäten Düsseldorf und Marburg (u.a. zum Thema „Medizinproduktehaftung“).

Im Ehrenamt ist Dr. Koyuncu Mitglied der Ethikkommission der Universität Dresden.

Agenda

- Rechtliche Einordnung
- Regulatorische Anforderungen an IT-/Cybersecurity bei Medizinprodukten
- Haftungsrisiken bei Defiziten der IT-/Cybersecurity – Wer haftet wann wofür?
  - Unternehmen
  - Geschäftsführung
  - Andere Verantwortliche (u.a. PRRC)

IT-/Cybersecurity-Risiken bei Medizinprodukten

$ 31.2 billion

Global market size of connected medical devices in 2021.[1] Projected to rise to $181.9B by 2030.[2]

48% 2018 **68%** 2023

Estimated percentage of connected medical devices[3]

10-15

Average number of connected medical devices per patient bed[4]

50+ million

Predicted number of patients monitored remotely in 2021[3]

53%

of connected medical devices and other IoT devices in hospitals had critical vulnerabilities as of Jan. 2021

6.2

vulnerabilities per medical devices on average in 2021

40%

of medical devices at end-of-life stage offer little to no security upgrades in 2021

[1, 2] Acumen Rsch. & Consulting, *Connected Medical Devices Market Is Expected To Reach US$ 181.9 Billion By 2030 - Exclusive Report By Acumen Research & Consulting* (June 13, 2022).
[3] Deloitte, *Medtech and the Internet of Medical Things*, at 13, 15 (July 2018)
[4] Heather Landi, *82% of healthcare organizations have experienced an IoT-focused cyberattack, survey finds*, Fierce Healthcare (Aug. 29, 2019)

IT-/Cybersecurity-Risiken bei Medizinprodukten


FORBES > INNOVATION > CYBERSECURITY

Medical Devices Hit By Ransomware For The First Time In US Hospitals

Thomas Brewster Forbes Staff

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Follow

May 17, 2017, 09:00am EDT

[WannaCry Ransomware Attack]

- Infected more than 230,000 computers in at least 150 countries within days of the attack in May 2017
- Affected radiological devices in some hospitals in the U.S.


SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication

Share Tweet LinkedIn Email Print

[SweynTooth Vulnerabilities (2020)]

- 12 vulnerabilities which would enable an unauthorized user to crash, deadlock, or bypass security of devices
- Affected several system-on-a-chip manufacturers, no adverse event yet

IT-/Cybersecurity-Risiken bei Medizinprodukten

IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft Journal

TOPTHEMEN: E-AUTO SECURITY WINDOWS 10 CORONAVIRUS MS FLIGHT SIMULATOR HOMEOFFICE

heise online › News › 09/2020 › **IT-Ausfall an Uniklinik Düsseldorf betrifft immer mehr Patienten**

IT-Ausfall an Uniklinik Düsseldorf betrifft immer mehr Patienten

Der IT-Ausfall an der Uniklinik Düsseldorf hat gravierende Folgen für immer mehr Patienten. Experten gehen von einem Hackerangriff aus.

Lesezeit: 1 Min. In Pocket speichern 130

(Bild: Billion Photos/Shutterstock.com)

15.09.2020 17:19 Uhr

Von dpa

WDR

Nachrichten Sport Wissen Verbraucher Kultur Unterhaltung

Uniklinik Düsseldorf: IT-Ausfall dauert möglicherweise noch Wochen

Nach dem Absturz des Computersystems könnte es noch Wochen dauern, bis das IT-System der Uniklinik Düsseldorf [illegible] einen Hackerangriff.

RP ONLINE NRW POLITIK SPORT PANORAMA KULTUR WIRTSCHAFT DIGITAL LEBEN MENÜ

RP+ IT-Ausfall mit gravierenden Folgen

Hunderte Eingriffe in der Uniklinik Düsseldorf fallen aus

17. September 2020 um 10:38 Uhr | Lesedauer: 2 Minuten

IT-/Cybersecurity-Risiken bei Medizinprodukten

Clinical Trials Hit by Ransomware Attack on Health Tech Firm

No patients were affected, but the incident was another reminder of the risks in the increasingly common assaults on computer networks.

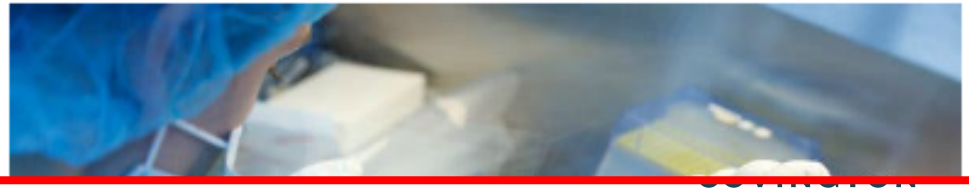
Published Oct. 3, 2020 Updated Oct. 4, 2020

A Philadelphia company that sells software used in hundreds of clinical trials, including the crash effort to develop tests, treatments and a vaccine for the coronavirus, was hit by a ransomware attack that has slowed some of those trials over the past two weeks.

The attack on eResearchTechnology, which has not previously been reported, began two weeks ago when employees discovered that they were locked out of their data by ransomware, an attack that holds victims' data hostage until they pay to unlock it. ERT said clinical trial patients were never at risk, but customers said the attack forced trial researchers to track their patients with pen and paper.

Russia Is Trying to Steal Virus Vaccine Data, Western Nations Say

The hackers have been targeting British, Canadian and American organizations racing to create coronavirus vaccines.



Published July 16, 2020 Updated Aug. 11, 2020

The New York Times

IT-/Cybersecurity bei Medizinprodukten – Regulatorische Anforderungen in der EU

Zusammenspiel mehrerer Regelwerke beachten (zuzüglich MDCG u.a. Guidelines und harmonis. Standards)

MDR / IVDR

Network and Information Security Directive ("NIS2")

DS-GVO

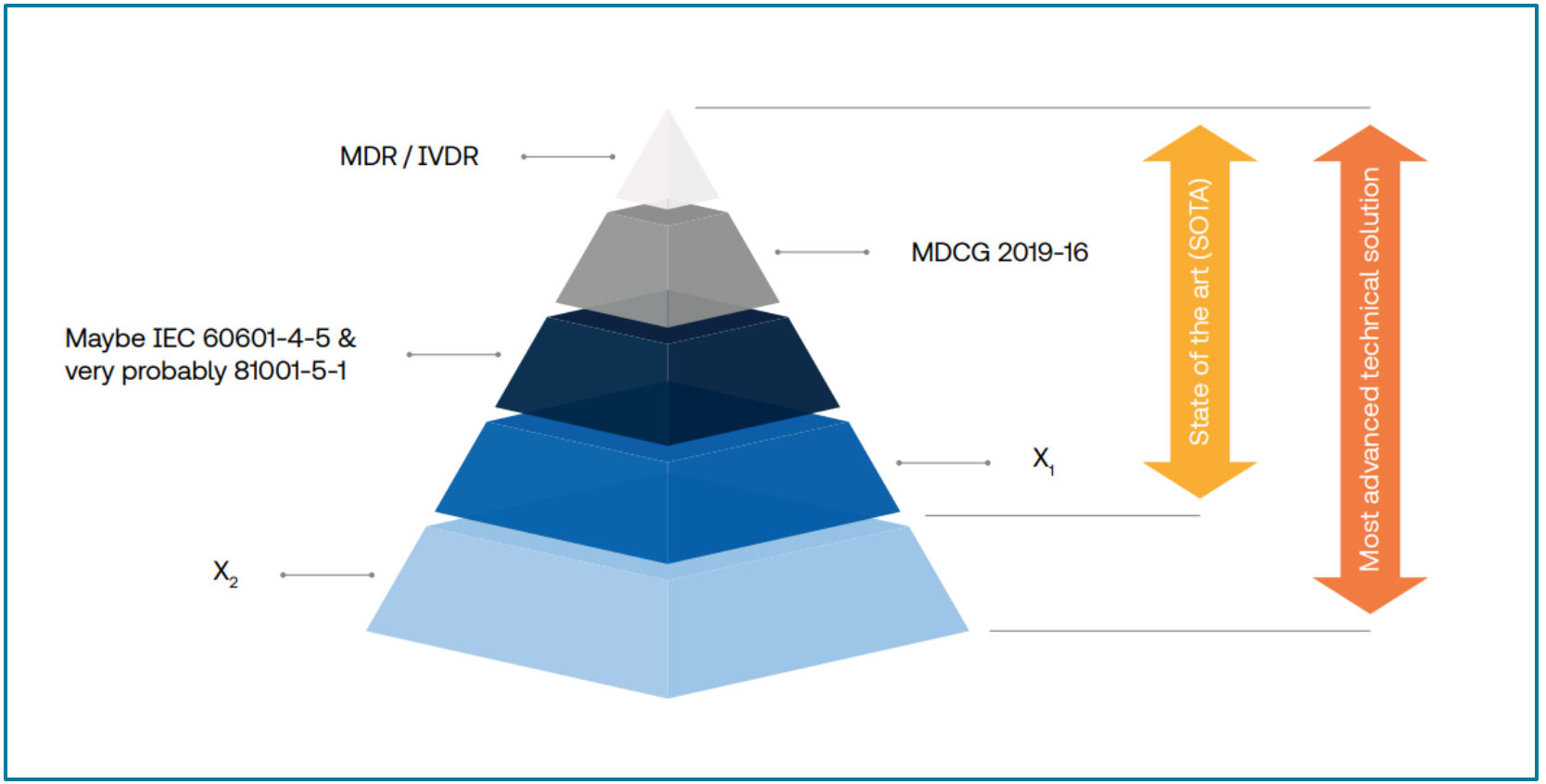
EU Artificial Intelligence Act

Data Act / EHDS

("Cyber Resilience Act")

IT-/Cybersecurity bei Medizinprodukten

Medizinprodukterechtliche Anforderungen



Quelle: TÜV SÜD, White Paper “Medical device cyber security“

IT-/Cybersecurity bei Medizinprodukten

Medical Device

Medical Device Coordination Group Document MDCG 2019-16 rev. 1

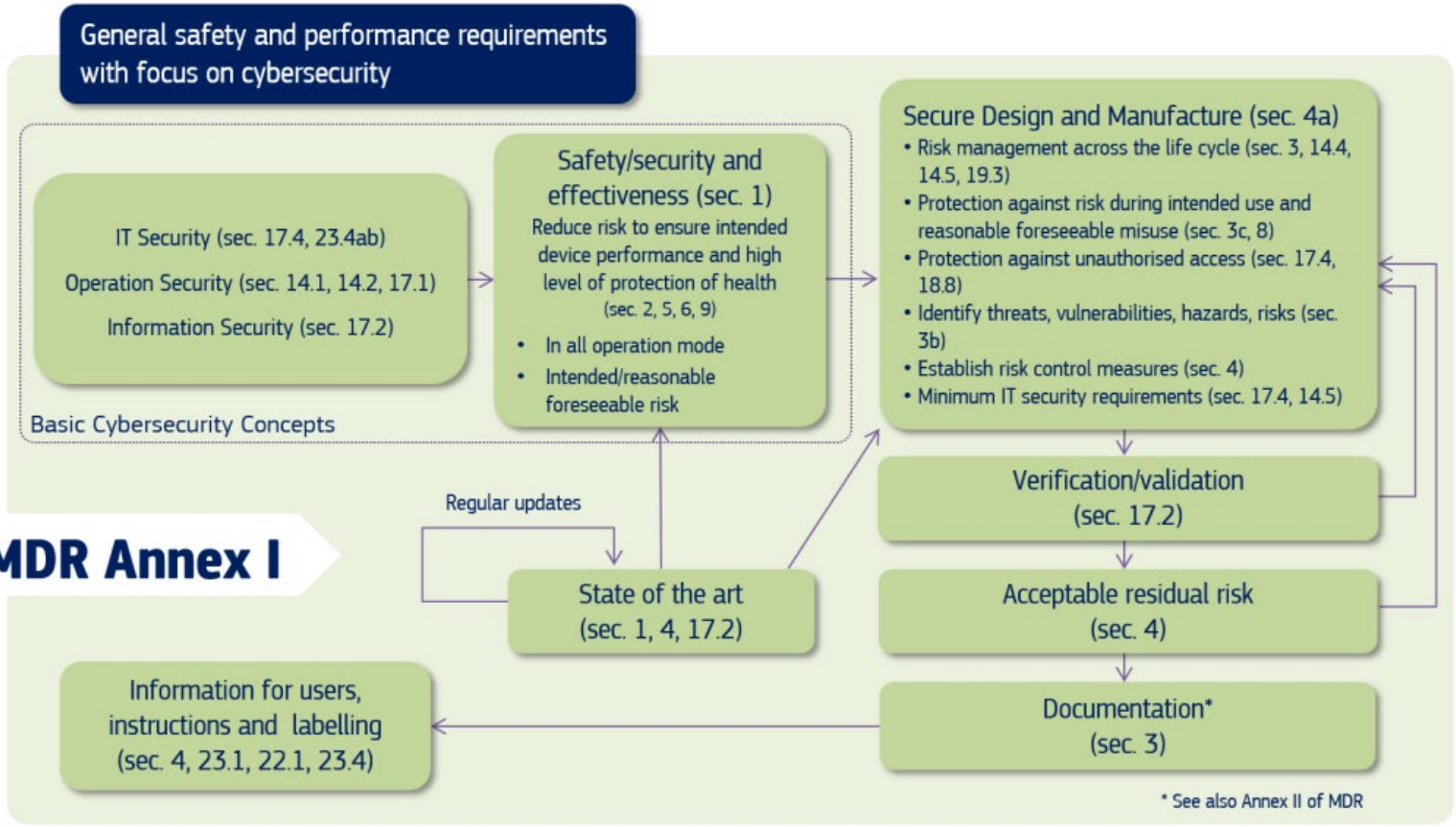


Figure 1: Cybersecurity requirements contained in MDR Annex I

IT-/Cybersecurity bei Medizinprodukten

Deutschland
Digital•Sicher•BSI•

Handlungsempfehlung für Hersteller von vernetzten Medizinprodukten

Version	*Datum*	*Name*	*Beschreibung*
Nummer			
1.0	14.02.2025	Referat D24	Initiale Veröffentlichung

IT-Sicherheit nach der NIS2-Richtlinie (1)

- NIS2: Ausweitung der EU-weiten Mindeststandards an Cybersicherheit
- Insbesondere mittlere und große Unternehmen erfasst
- Erhöhte Anforderungen an Cyber- und Informationssicherheit für besonders wichtige und wichtige Einrichtungen
- Umsetzung in nationales Recht (Frist: 17. Oktober 2024 – ursprünglich Umsetzung vorgesehen durch „BSIG-E“)

IT-Sicherheit nach der NIS2-Richtlinie (2)

Anwendungsbereich

Besonders wichtige Einrichtungen (Sektoren hoher Kritikalität)

- Betreiber kritischer Anlagen: Energie-, Bank-, Wasser-, Transport-, und Gesundheitswesen (u.a. bestimmte pharmazeut. Betriebe und Hersteller von Medizinprodukten für Notlagen)
- Unternehmen ab 250 Mitarbeiter oder über 50 Mio EUR Umsatz (Anlage 1)

Sonstige kritische Sektoren

- Unternehmen ab 50 Mitarbeiter oder über 10 Mio EUR Umsatz (Anlage 1, 2)
- Verarbeitendes Gewerbe/Herstellung von Waren: … Medizinprodukte und In-vitro-Diagnostika

- Gleiche Pflichten für beide Einrichtungen im Bereich Datensicherheit und Meldungen von Vorfällen
- Strengere Durchsetzungsmechanismen für besonders wichtige Einrichtungen

IT-Sicherheit nach der NIS2-Richtlinie (3)

Pflichten nach der NIS2-Richtlinie

- Risikomanagementmaßnahmen für die Sicherheit der Netz- und Informationssysteme und zur Geringhaltung von Sicherheitsvorfällen (Art. 21 (1) NIS-2)
- Maßnahmen technischer, betrieblicher und organisatorischer Art
- Sicherheitsniveau muss angemessen zum bestehenden Risiko sein
- Berücksichtigung des Stands der Technik
- Identifizierung der Gefahren für Lieferketten und Gewährleistung der Sicherheit der Lieferkette
- Informations- und Meldepflichten

IT-Sicherheit nach der NIS2-Richtlinie (4)

Umgang mit Sicherheitsvorfällen:

Meldepflicht gegenüber Aufsichtsbehörde (Art. 23 (1), (4) und betroffene Empfänger (Art. 23 (2) NIS-2 / §§ 32, 35 BSIG-E)

Zusammenspiel mit DS-GVO bei Sicherheitsvorfall:

Ggfs. Meldepflichten nach Art. 33 und 34 DS-GVO

Haftungsrisiken bei Defiziten der IT-/Cybersecurity

Wer haftet für Schäden infolge von Cyber-Attacken bzw.

IT-Security-Defiziten?

Haftungsrisiken bei Defiziten der IT-/Cybersecurity

Nach welchen Regeln haften die Beteiligten?

- Vertragliche Gewährleistungshaftung
- Vertragliche Schadensersatzhaftung
- Haftung nach dem Produkthaftungsgesetz (unabhängig von Verschulden)
- Haftung nach § 823 ff. BGB (abhängig von Verschulden)
- Haftung nach DS-GVO und NIS2-Richtlinie (bzw. ihrer nationalen Umsetzung)

Haftungsrisiken bei Defiziten der IT-/Cybersecurity

Verschuldensunabhängige *Produkt*haftung nach § 1 ProdHaftG

- Umsetzung der EU-Produkthaftungsrichtlinie
- Haftung ohne Verschulden

- Haftungstatbestand § 1 Abs. 1 S. 1 ProdHaftG:
  - „*Wird durch den Fehler eines Produkts jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Hersteller des Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen.*“

Haftungsrisiken bei Defiziten der IT-/Cybersecurity

Vorliegen eines Fehlers gemäß § 3 ProdHaftG

- Abs. 1: *„Ein Produkt hat einen Fehler, wenn es nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände, insbesondere*

  a) seiner Darbietung,

  b) des Gebrauchs, mit dem billigerweise gerechnet werden kann,

  c) des Zeitpunkts, in dem es in den Verkehr gebracht wurde,

  berechtigterweise erwartet werden kann.“

- Entscheidend: „berechtigte Sicherheitserwartung“:
  - Ermittlung der berechtigten Sicherheitserwartung anhand der Wertung und Betrachtung aller Umstände des Einzelfalls.
  - Beim Einsatz von MP bestehen grds. hohe Sicherheitserwartungen

Haftungsrisiken bei Defiziten der IT-/Cybersecurity

§ 3 ProdHaftG – Darbietung des Medizinprodukts

- Unter Darbietung versteht man die Gesamtheit aller Umstände, unter denen das Produkt vom Hersteller in den Verkehr gebracht wird und durch welche die Sicherheitserwartungen vorgegeben oder beeinflusst werden.
- Dies umfasst die Zweckbestimmung, Produktbeschreibungen, Webeaussagen, Gebrauchsanleitungen, Verpackung, und Warnhinweise
  - Sicherheitsrelevante Werbeaussagen können das Haftungsrisiko des Herstellers erhöhen
- Maßgeblich ist der durchschnittliche Erfahrungs- und Kenntnisstand des jeweiligen Benutzerkreises

Haftungsrisiken bei Defiziten der IT-/Cybersecurity

Neue EU-Produkthaftungsrichtlinie 2024/2853

- Erhebliche Neuerungen
- Erweiterung der erfassten Produkte auf Software und den digitalen Bereich
- Erweiterung der Definition eines Produktfehlers
  - Unternehmen können künftig für Schäden durch fehlende oder unzureichende **Softwareupdates** oder schwachen **Cybersecurity-Schutz** haften.
- Neue Auskunftsansprüche für Kläger und Offenlegungspflichten für Hersteller
- Neue Vermutungsregelungen für wichtige Beweisfragen

- Nationale Implementierung steht aus (Frist: 9. Dezember 2026)

Haftungsrisiken bei Defiziten der IT-/Cybersecurity

§ 823 Abs. 1 BGB - Allgemeine Verschuldenshaftung

- *„Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.“*
- Haftung für Verkehrssicherungspflichten: Hersteller ist verpflichtet, in den Grenzen des technisch Möglichen und wirtschaftlich Zumutbaren dafür Sorge zu tragen, dass Dritte durch seine Produkte nicht geschädigt werden.
- Kein Haftungshöchstbetrag;
- Haftung nicht begrenzt auf Hersteller → jeder Schadensverursacher kann hier unbegrenzt haften

Haftungsrisiken bei Defiziten der IT-/Cybersecurity

Persönliche Haftung *vs.* Unternehmenshaftung

- Persönliche Haftung z.B. der Geschäftsführer eines Unternehmens verläuft nach anderen rechtlichen Voraussetzungen
- Rechtliche Voraussetzungen für persönliche Haftung sind strenger als die der Unternehmenshaftung
  - Abhängig von persönlicher Pflichtverletzung und
  - abhängig von persönlichem Verschulden

Aber: Risiko „Garantenstellung“ (u.a. von Geschäftsführung, Vorstand oder Beauftragten wie zB bestimmte „Beauftragte“ im Unternehmen oder PRRCs

IT-Security, Risk Management & Produkthaftung – Rechtliche Einordnung

Fragen oder Anmerkungen?

Referent:

Dr. iur. Dr. med. Adem Koyuncu
Rechtsanwalt und Arzt

- Mitglied im „Arbeitskreis Recht“ des BVMed und im „Rechtsausschuss“ von Pharma Deutschland e.V.
- Lehrbeauftragter der Universitäten Düsseldorf und Marburg

Partner der Kanzlei Covington & Burling LLP
Taunusanlage 9-10, 60329 Frankfurt am Main
Bolwerklaan 21, 1210 Brüssel
T +49 69 76806-3366
E: akoyuncu@cov.com
www.cov.com