

# Künstliche Intelligenz trifft Medical Device Regulation Algorithmen als regulatorische Herausforderung zwischen MDR und AI-Act

- KI und datenschutzrechtliche Aspekte -

23. Juni 2026

Walburga van Hövell, LL.M. (Medizinrecht)

## Agenda

### 1. **Datenschutzanforderungen bzgl. Entwicklung und Einsatz von KI in der Medizin(technik)**

- Wann gilt die DSGVO?
- Wissenswertes und Grundsätze der DSGVO
- DSGVO-Erlaubnistatbestände inkl. Besonderheiten im medizinischen Kontext
- (Zukünftige) Datenquellen
- Automatisierte Entscheidungsfindung gem. Art. 22 DSGVO

### 2. **Hersteller- und Betreiber-Haftung bzgl. KI**

- Neues zur Produkthaftung nach dem Entwurf der Bundesregierung zur Modernisierung des Produkthaftungsgesetzes
- Produzentenhaftung
- Haftung aufgrund Verletzung eines Schutzgesetzes
- Betreiberhaftung

# 1. Datenschutzerfordernissen bzgl. Entwicklung und Einsatz von KI in der Medizin(technik)



## Wann gilt die DSGVO (im medizinischen Kontext)?

- Sachlicher Anwendungsbereich ergibt sich aus Art. 2 DSGVO:  
→ **Verarbeitung personenbezogene Daten!**
- Wichtige Begriffsdefinitionen finden sich Art. 4 DSGVO:
  - Nr. 1: personenbezogene Daten<sup>1</sup>
  - Nr. 2: Verarbeitung
  - Nr. 7: Verantwortlicher
  - Nr. 13: genetische Daten
  - Nr. 14: biometrische Daten
  - Nr. 15: Gesundheitsdaten sind *„personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.“*

## Beispiele Gesundheitsdaten (I)

→ Der Begriff Gesundheitsdaten ist grundsätzlich weit zu verstehen!

- Krankengeschichte (Anamnese)
- Informationen über aktuelle Erkrankungen, Diagnosen, Behandlungen, Therapien und deren Verlauf
- Informationen zu chronischen Erkrankungen, Vorerkrankungen, Allergien, Unverträglichkeiten
- Andere gesundheitsbezogene Informationen (z.B. Körperfettwerte, Blutzuckerwerte)
- Informationen zum Impfstatus
- Medikamentierung
- Laborergebnisse
- Bildgebung (z.B. MRT, Röntgenbilder)
- Im weitesten Sinne auch: Informationen zum Versichertenstatus, Arztrechnungen, Arzttermine etc.



## Beispiele Gesundheitsdaten (II)

→ Der Begriff der „Gesundheitsdaten“ ist wirklich weit zu verstehen!

Deutsches  
Arzteblatt



Menschlicher Oberschenkelknochen inklusive Hüftkopfprothese /Polizeipräsidium Südosthessen

Berlin/Mainz-Kinzig – Das Polizeipräsidium Südosthessen, Polizeidirektion Main-Kinzig, sucht seit dem vergangenen Jahr nach Hinweisen zu einer gefundenen Hüftkopfprothese. Bisher offenbar ohne Erfolg. Nun wenden sich die Kriminalisten erneut an die Ärzteschaft und bitten um Mithilfe.

Auf einem Schrottplatz in Langenselbold war bereits am 16. Februar ein menschlicher Oberschenkelknochen inklusive Hüftkopfprothese gefunden worden. Der Knochen ist 38 cm lang, rechtsseitig und von einem Mann. Ein Gewaltverbrechen kann nicht ausgeschlossen werden.

## Wann gilt die DSGVO (im medizinischen Kontext) nicht?

- DSGVO-Erwägungsgrund **26**:
  - **Satz 1:** „Die Grundsätze des Datenschutzes sollten für *alle Informationen* gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.“
  - **Satz 2:** „Einer *Pseudonymisierung* unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden.“
  - **Satz 6:** „Diese Verordnung betrifft somit *nicht die Verarbeitung solcher anonymer Daten*, auch für statistische oder für Forschungszwecke.“

## Wer ist für die Einhaltung der DSGVO verantwortlich?

- Art. 4 Nr. 7 DSGVO: „*Verantwortlicher*“ ist „*die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (...)*.“
- Ausnahmen in Art. 2 Abs. 2 DSGVO definiert (z.B. *keine DSGVO-Anwendung auf natürliche Personen bzgl. deren Verarbeitung zu ausschließlich persönlichen oder familiären Zwecken*).
- **Problem:** Was passiert, wenn KI – und damit weder eine natürliche oder juristische Person – autonom über Zwecke und Mittel der personenbezogenen Datenverarbeitung entscheidet?
  - (unausgegrenzte) Ideen für die Zukunft: „e-Person“ und/oder „Fondlösung“

## Was ist alles Datenverarbeitung?

- Art. 4 Nr. 2 DSGVO: „*Verarbeitung*“ ist jede „*mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung*“
- Beispiele:
  - Dokumentation, z.B. bzgl. Behandlung oder im Rahmen von klinischen Studien
  - (elektronischer) Datentransfer, aber auch analoges Versenden von personenbezogenen Daten
  - Aufnahme und Archivierung von Bildgebung (wenn Personenbezug vorhanden)
  - Training von KI-Modellen
  - Datenauswertung im Rahmen von KI-Anwendung
  - **Cave: Die Bundesdatenschutzbeauftragte (BfDI) vertritt die Auffassung, dass es sich bei der Anonymisierung von personenbezogenen Daten um eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO handelt!**

## **Bzgl. jeder Verarbeitung personenbezogener Daten gelten die Grundsätze des Art. 5 DSGVO**

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
2. Zweckbindung
3. Datenminimierung
4. Richtigkeit der Daten
5. Speicherbegrenzung
6. Integrität und Vertraulichkeit (Sicherheit der Verarbeitung)
7. Rechenschaftspflicht

## DSGVO-Erlaubnistatbestände

- Grds. gelten Erlaubnistatbestände des Art. 6 DSGVO (u.a. Einwilligung, Vertragserfüllung oder berechtigtes Interesse)
- Ausnahme nach Art. 9 Abs. 1 DSGVO bzgl. der sog. sensiblen Daten wie z.B. Gesundheitsdaten, hier ist die Datenverarbeitung untersagt, außer, die Datenverarbeitung ist nach Abs. 2 erlaubt.
- *Spoiler:* Berechtigtes Interesse nach Art. 6 Abs. 1 lit. f) DSGVO ist kein Erlaubnistatbestand i.S. des Art. 9 Abs. 2 DSGVO – a.A. OLG Köln im Zusammenhang mit KI-Datenverarbeitung durch Meta, Beschluss vom 23.5.2023, Az. 15 UKI 2/25, Rz. 120 („In der KI-VO hat der europäische Gesetzgeber zudem in Kenntnis der Notwendigkeit des Trainings generativer KI mittels großer Massen an Daten (...) und in Kenntnis der seit längerem erfolgenden Nutzung von Webscraping zur Gewinnung von KI-Trainingsdaten, das stets die Gefahr der – unbeabsichtigten und nicht zielgerichteten – Verarbeitung von Daten im Sinne des Art. 9 DSGVO birgt, Öffnungsregelungen, die ein Training von KI mit Massendaten erlauben, nicht getroffen. Dies lässt sich aus Sicht des Senats nicht anderes verstehen, als dass der Gesetzgeber nicht von einer entsprechenden Unmöglichkeit oder grundsätzlichen Rechtswidrigkeit ausgegangen ist.“)

## Ausnahme-(Erlaubnis-)tatbestände (im medizinischen Kontext) des Art. 9 Abs. 2 DSGVO (I)

- **Lit. a):** Die ausdrückliche Einwilligung für einen oder mehrere festgelegte Zwecke
  - Problem 1: Praktikabilität
  - Problem 2: Widerruf der Einwilligung (*mögliche Lösung Art. 17 Abs. 3 lit. c DSGVO: Keine Löschpflicht bei Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, aber nur wenn Verarbeitung durch Fachpersonal mit Verpflichtung zum Berufsgeheimnis i.S. des Art. 9 Abs. 3 DSGVO*)
  - Problem 3: Zweckänderung der Datenverarbeitung. *Mögliche Lösungsansätze:*
    - Broad Consent: Einwilligung wird nur bzgl. abstrakt beschriebener Verarbeitungszwecke und technischer Prozesse eingeholt.
      - **Bzgl. Forschungszwecken** i.S. des DSGVO-ErwGr. 33 **möglich**.
      - *Problematisch, wenn der Forschungszweck entfällt. Mögliche Argumentation bzgl. Entwicklung und Einsatz künstlich lernender Medizinprodukte könnte im Einzelfall Bezugnahme auf ErwGr. 159 S. 2 DSGVO sein, **wonach Datenverarbeitung zu wissenschaftlichen Forschungszwecken inkl. der privat finanzierten Forschung weit ausgelegt werden und die Verarbeitung für beispielsweise technologische Entwicklungen einschließen soll.***
    - Dynamic Consent: Verantwortlicher soll Verarbeitungszwecke bzgl. einer bereits erteilten Einwilligung erweitern können, wenn die Betroffenen über die angepassten Verarbeitungszwecke fortlaufend informiert werden und entscheiden können, ob sie ihre Einwilligung unter den geänderten Bedingungen widerrufen wollen.

## Ausnahme-(Erlaubnis-)tatbestände (im medizinischen Kontext) des Art. 9 Abs. 2 DSGVO (II)

- **Lit. h): Maßnahmen für individuelle Versorgung im Gesundheitsbereich**
  - Art. 9 Abs. 2 lit. h ist der datenschutzrechtliche **Erlaubnistatbestand bzgl. ärztlicher KI-Anwendung im Behandlungskontext** (z.B. Entscheidungsunterstützung durch KI-basierte Diagnostiksysteme)
  - **Zusätzliche Rechtsgrundlage** wie spezielles Gesetz oder Vertrag ist notwendig (z.B. Behandlungsvertrag)
  - Einschlägige **Berufsgeheimnisse**: Verschwiegenheitspflicht Ärzte aus BO (Einbindung von nichtärztlichen Mitarbeitern i.S. § 203 StGB notwendig), Sozialgeheimnis gem. § 35 SGB I für KK-/PflegeK-Mitarbeiter
  - *CAVE: Kein Erlaubnistatbestand, wenn Datenverarbeitung nicht für den normativ geforderten konkreten medizinischen Behandlungs- oder sozialrechtlichen Kontext erforderlich ist. D.h., Art. 9 Abs. 2 lit. h) ist kein datenschutzrechtlicher Erlaubnistatbestand für die Entwicklung von KI-basierten Medizinprodukten.*

## Ausnahme-(Erlaubnis-)tatbestände (im medizinischen Kontext) des Art. 9 Abs. 2 DSGVO (III)

- **Lit. i): öffentliche Gesundheitsbelange** (z.B. öffentliches Interesse an Gewährleistung hoher Qualitäts- und Sicherheitsstandards von Medizinprodukten) + **grundlegende gesetzliche Regelung**
  - **Öffentliche Gesundheit:** Kann weit ausgelegt werden.
  - **Erforderlichkeit:** Die Datenverarbeitung muss zwingend notwendig sein, um den Zweck des öffentlichen Interesses zu erreichen.
  - **Zusätzliche Rechtsgrundlage:** Das erforderliche Gesetz muss angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Personen enthalten, insbesondere ein Berufsgeheimnis.
  - **Bsp. für Rechtsgrundlagen:**
    - § 363 SGB V (Verarbeitung von Daten der ePA zu Forschungszwecken)
    - § 4 GDNG (Verknüpfung von Daten des Forschungsdatenzentrums Gesundheit mit Daten der klinischen Krebsregister der Länder).

## Ausnahme-(Erlaubnis-)tatbestände (im medizinischen Kontext) des Art. 9 Abs. 2 DSGVO (IV)

- **Lit. j): Archivzwecke, wissenschaftliche und historische Forschungszwecke, statistische Zwecke**
  - **Zweckbindung** : Die Datenverarbeitung muss zwingend für archivarische, wissenschaftliche oder statistische Zwecke erfolgen.
  - **Öffentliches Interesse:** (z.B. Gesundheitsschutz zum Wohl der Allgemeinheit) ist in jedem Fall erforderlich, aber wann liegt es vor? Im Einzelfall muss das öffentliche Interesse gut argumentiert werden können, v.a., wenn auch kommerzielle Interessen mitspielen...
  - Nach DSGVO-ErwGr. 159 ist der Begriff der wissenschaftlichen Forschung weit zu verstehen.
  - **Zusätzliche Rechtsgrundlage:** Die Verarbeitung muss auf Grundlage eines Gesetzes zulässig sein:
    - z.B. § 25 Landeskrankenhausgesetz Berlin: Verarbeitung von genetischen Daten und Gesundheitsdaten zu wissenschaftlichen Forschungszwecken ist unter bestimmten Umständen ohne Einwilligung zulässig; ABER Ärztevorbehalt bzgl. der Datennutzung und eine gewerbliche Nutzung ist ausdrücklich ausgeschlossen).

## Ausnahme-(Erlaubnis-)tatbestände (im medizinischen Kontext) des Art. 9 Abs. 2 DSGVO (V) – der Blick in die mögliche Zukunft

- Art. 3 Nr. 3 Vorschlag COM(2025) 837 der EU-Kommission (zur DSGVO-Anpassung im Rahmen des „Digitalen Omnibus“):
  - **Erweiterung des Art. 9 DSGVO um einen Erlaubnistatbestand für Training und Betrieb von KI-Anwendungen**, allerdings unter strengen Auflagen:
    - Pflicht zu technischen und organisatorischen Maßnahmen, um **besonders geschützte Daten vom KI-Training/-Betrieb auszuschließen**.
    - Werden solche Daten dennoch erfasst, besteht eine **Pflicht zu deren Entfernung**.
    - **Ausnahme** von der Entfernung **nur bei unverhältnismäßigem Aufwand und nur bei zusätzlichen Schutzmaßnahmen**.

## Gibt es nicht auch einen datenschutzrechtlichen Erlaubnistatbestand in der KI-VO?

- Ja, **Art. 10 Abs. 5**, bzgl. Hochrisiko-KI und der Verarbeitung sensibler personenbezogener Daten zur Erkennung und Korrektur von Verzerrungen (Bias)
  - **Grundsatz:** Art. 10 Abs. 5 KI-VO ist eine Ausnahme vom generellen Verbot der Verarbeitung sensibler Daten, sofern dies zwingend zur Gewährleistung der Sicherheit und Grundrechte erforderlich ist.
  - **Zwingende Erforderlichkeit:** Die Verarbeitung (Bias-Erkennung/Korrektur) muss unbedingt notwendig sein, um Verzerrungen zu verhindern.
  - **Einzuhaltende Datenschutz-Garantien:** Pseudonymisierung, keine Datenübermittlung an Dritte, Datenlöschung nach Zweckerreichung (Bias-Korrektur)
  - **Technische und organisatorische Maßnahmen:** Es müssen hohe Sicherheitsstandards eingehalten werden.
  - **Dokumentation:** Die Verarbeitung muss dokumentiert werden, um die Einhaltung gegenüber Behörden nachweisen zu können.

## (Zukünftige) Datenquellen

- **Die elektronische Patientenakte (ePA):**
  - Dort gespeicherte Daten von gesetzlich Versicherten sollen entsprechend Gesundheitsdatennutzungsgesetz (GDNG) und spezieller SGB V-Vorschriften (z.B. § 363) auch der Forschung bzw. mit Einwilligung der Versicherten der Nutzung durch Krankenkassen (§ 345) dienen.
  - Gesundheitsdaten aus der ePA fließen *pseudonymisiert* an das Anfang Oktober 2025 gegründete Forschungsdatenzentrum (FDZ) beim BfArM. Forschende können die Nutzung unter <https://www.forschungsdatenzentrum-gesundheit.de/antragstellung> beantragen, vorausgesetzt, ein Nutzungszweck i.S. des § 303e Abs. 2 SGB V muss angegeben werden (z.B. Nutzenbewertung von Arzneimitteln, Medizinprodukten, Untersuchungs- und Behandlungsmethoden).

Anträge zur Entwicklung, Weiterentwicklung von Systemen der Künstlichen Intelligenz im Gesundheitswesen stellen besondere Herausforderungen an Hardware, Software, Trainingsdaten und publizierbare Ergebnismengen. Um die Realisierbarkeit und Erfolgsaussichten für Anträge mit diesem Auswertungszweck einschätzen zu können, wenden Sie sich bitte vor der Antragseinreichung an das FDZ.

- **European Health Data Space (EHDS):**
  - Stufenweise einzuführender einheitlicher europäischer Rechtsrahmen für die Verarbeitung von Gesundheitsdaten der EU-Bürger.
  - Primärnutzung: Patienten sollen ihre elektronischen Gesundheitsdaten (wie E-Rezepte oder Entlassbriefe) sicher und einfach EU-weit einsehen und mit medizinischem Fachpersonal teilen können.
  - Sekundärnutzung: Gesundheitsdaten können unter strengen Datenschutzauflagen anonymisiert und für wissenschaftliche Forschung, die Entwicklung neuer Medikamente oder die Planung des Gesundheitswesens genutzt werden.
  - **Hauptanwendungsbeginn erst 2029**

## Die automatisierte Entscheidungsfindung gem. Art. 22 DSGVO

- Grundsätzlich dürfen Entscheidungen mit Rechtswirkung oder in ähnlich beeinträchtigender Weise nur von Menschen getroffen werden.
- Was aber, wenn ein KI-basiertes Medizinprodukt dazu genutzt wird, diagnostische oder therapeutische Entscheidungen zu treffen, und diese Entscheidungen ohne weitere menschliche Kontrolle umgesetzt würden?
  - Grds. bedarf es bei automatisierter Entscheidungsfindung einer Rechtsgrundlage!
  - Bzgl. besonders sensibler Daten wie Gesundheitsdaten bedarf es einer Einwilligung, vgl. Art. 22 Abs. 4 i.V.m. Art. 9 Abs. 2 lit. a) DSGVO!
  - **Problem Arztvorbehalt (mehr als nur „human factor in the loop“)**: Medizinische Tätigkeiten einschl. Diagnose oder Therapieanwendung darf nur ein approbierter Arzt bzw. in bestimmten Fällen ein Heilpraktiker oder eine Pflegefachperson ausüben. Die Delegation ärztlicher Leistungen ist nur in engen normativen Rahmen erlaubt und bislang nur an entsprechend qualifiziertes Personal [≠ KI].

## Abschlussquiz zum Datenschutz



## Exkurs: Ärztliches Berufsrecht und Schweigepflicht im KI-Kontext

- **Ärztliche Verantwortung/“Human/Doctor in the Loop“**
  - Der behandelnde Arzt trägt stets die Behandlungshoheit sowie-verantwortung und damit die alleinige Letztentscheidungsbefugnis im Behandlungskontext (ergibt sich aus § 1 Heilpraktikergesetz [Arztvorbehalt bzgl. Ausübung Heilkunde], §§ 2 Abs. 2, 11 Abs. 1 [gewissenhafte Berufsausübung und Versorgung], Art. 14 KI-VO [Menschliche Aufsicht bzgl. Hochrisiko-KI]).
  - Eine vollständige Delegation von Diagnostik oder Therapieentscheidungen an ein autonomes System ist berufsrechtlich unzulässig.

## Exkurs: Ärztliches Berufsrecht und Schweigepflicht im KI-Kontext

- **Zentrale berufsrechtliche Pflichten, aus denen bestimmte Vorgaben für KI-Nutzung abgeleitet werden können:**
  - **Facharztstandard (§ 630a Abs. 2 BGB):** Ärzte müssen KI-Vorschläge stets plausibilisieren, blindes Vertrauen unterläuft Facharztstandard. Allerdings könnte sich bzgl. bestimmter Behandlungen und Diagnosen die KI-Unterstützung zum Facharztstandard entwickeln. Kann ein Arzt das nicht anbieten, dann muss hierüber aufgeklärt werden und Patient muss in alten Standard einwilligen, ggf. muss Patient auch an Behandler weiterverwiesen werden, der über nötiges KI-Tool verfügt. Bzgl. KI-Neulandmethoden bedarf es ebenfalls entsprechender Aufklärung und Einwilligung.
  - **Fernbehandlung (§ 7 Abs. 4 MBO-Ä):** KI-basierte Kommunikationsmedien dürfen den persönlichen Arzt-/Patienten-Kontakt unterstützen, aber nicht ersetzen
  - **Fortbildungspflicht (§ 4 Abs. 1 MBO-Ä) & KI-Kompetenz (Art. 4 KI-VO, aber ggf. Abschwächung durch "Digital Omnibus"):** Ärzte sind verpflichtet, sich über die Funktionsweise, Grenzen und Risiken der genutzten KI-Systeme fortzubilden, um eine sichere Anwendung und Überwachung zu gewährleisten.
  - **Aufklärungspflicht (§ 630e BGB) zum KI-Einsatz:** Patienten müssen transparent informiert werden, wenn wesentliche klinische Entscheidungen oder Diagnosen maßgeblich durch Algorithmen gestützt werden.
  - **Haftpflichtversicherung (§ 21 MBO-Ä):** Der Einsatz innovativer KI-Systeme in der Praxis muss zwingend mit der eigenen Berufshaftpflichtversicherung abgestimmt werden.

## Exkurs: Ärztliches Berufsrecht und Schweigepflicht im KI-Kontext

- Die Frage nach der ärztlichen Schweigepflicht im KI-Kontext stellt sich, wenn im Rahmen der ärztlichen Berufsausübung z.B. Mitarbeiter eines Medizinprodukte-Herstellers Zugriff auf Patientengeheimnisse erhalten soll.
- Der Umfang ärztlichen Schweigepflicht ist nach § 9 MBO-Ä mit Ausnahme offenkundiger oder bedeutungsloser Tatsachen sehr weit zu verstehen.
- Der Verstoß gegen die ärztliche Schweigepflicht ist nach § 203 StGB strafbar!
- Tathandlung ist das „Offenbaren“ eines Geheimnisses an einen Dritten. Dritter ist grundsätzlich jedermann (≠ KI), unabhängig davon, ob er selbst zur Verschwiegenheit verpflichtet ist.
  - Um straffrei zu bleiben ist Einbindung in die ärztliche Schweigepflicht nötig .
  - Bei ordnungsgemäß (schriftlich! § 9 Abs. 4 MBO-Ä) eingebundenen berufsmäßig tätigen Gehilfen liegt nach § 203 Abs. 3 StGB keine Offenbarung des Geheimnisses vor (→Alternative: Patient entbindet wirksam von der ärztlichen Schweigepflicht).

## 2. Hersteller- und Betreiber-Haftung bzgl. KI



## Regierungsentwurf eines Gesetzes zur Modernisierung des Produkthaftungsrechts vom 17.12.2025

### 1. Der Produktbegriff (§ 2):

- **Abs. 1:**
  - Als Produkt gilt jede bewegliche Sache (einschließlich Rohstoffen) sowie Elektrizität.
  - Auch sämtliche Arten von Software (inklusive KI-Systeme, Cloud-Anwendungen und Apps) sowie digitale Konstruktionsunterlagen (z. B. CAD-Dateien) gelten nun explizit als Produkt
- **Abs. 2:**
  - Es ist unerheblich, ob das Produkt in ein anderes Produkt oder in eine unbewegliche Sache integriert oder damit verbunden ist.

## Regierungsentwurf eines Gesetzes zur Modernisierung des Produkthaftungsrechts vom 17.12.2025

### 2. Bisher hafteten im Produkt der tatsächliche Hersteller, der Importeur in die EU, der „Quasi-Hersteller“ und ausnahmsweise der Händler. Dazu kommen nun:

- **Der Komponentenhersteller:** Wer eine fehlerhafte Komponente (inklusive Software-Updates oder verbundene digitale Dienste) herstellt, die mit Einverständnis des Hauptherstellers integriert wurde (§ 4 Abs. 1).
- **Der Umgestalter („Upcycler“):** Wer ein bereits in Verkehr gebrachtes Produkt ohne Einverständnis des ursprünglichen Herstellers *wesentlich verändert* und anschließend wieder auf dem Markt bereitstellt (§ 5 Abs. 1).
- **Der Bevollmächtigte (Beauftragte):** Wer vom außerhalb der EU ansässigen Hersteller schriftlich beauftragt wurde, in dessen Namen bestimmte Aufgaben wahrzunehmen (§ 10 Nr. 2).
- **Der Fulfillment-Dienstleister:** Wer (sofern kein EU-Hersteller, Importeur oder Beauftragter ermittelt werden kann) Dienstleistungen wie Lagerhaltung, Verpackung oder Adressierung anbietet, ohne Eigentümer des Produkts zu sein (§ 11).
- **Online-Marktplätze (Plattformbetreiber):** Sie werden im Entwurf unter bestimmten Voraussetzungen wie Lieferanten behandelt, wenn sie dem Verbraucher gegenüber den Eindruck erwecken, das Produkt selbst oder unter eigener Aufsicht bereitzustellen (§ 13).

## Regierungsentwurf eines Gesetzes zur Modernisierung des Produkthaftungsrechts vom 17.12.2025

### 3. Erweiterungen der Fehlerhaftigkeit eines Produkts :

- Grds. ist ein Produkt i.S. des § 7 S. 1 fehlerhaft, wenn es entweder gegen gesetzliche Sicherheitsvorschriften (deutsches oder EU-Recht) verstößt oder nicht die Sicherheit bietet, die berechtigterweise erwartet werden darf.
- **S. 2, Einbeziehung u.a. folgender Kriterien in Grundannahme der Fehlerhaftigkeit:**
  - **Nr. 3 "lernende" Produkte/KI**, die Selbstlernfähigkeiten eines Produkts nach dem Kauf (z. B. eine KI, die durch fehlerhaftes Training ein unvorhersehbares, gefährliches Verhalten entwickelt) fließen direkt in die Fehlerbewertung ein.
  - **Nr. 4, Wechselwirkungen im Ökosystem:** Ein Produkt kann künftig als fehlerhaft eingestuft werden, wenn es im *vorhersehbaren Zusammenspiel* mit anderen Geräten oder digitalen Diensten zu einer Gefahr führt (z.B. durch fehlerhafte Updates)
  - **Nr. 5.: Cybersicherheit**

## Regierungsentwurf eines Gesetzes zur Modernisierung des Produkthaftungsrechts vom 17.12.2025

### 4. Neuerungen zum Schaden, der grds. in § 1 geregelt ist:

- **Abs. 1 Nr. 1, Klarstellung bzgl. psychischer Schäden:** Medizinisch anerkannte Beeinträchtigungen der psychischen Gesundheit werden im Gesetzestext explizit mit körperlichen Schäden gleichgestellt
- **Abs. 1 Nr. 3 Ersatz von Datenverlust:** Die Vernichtung oder Beschädigung von privat genutzten Daten gilt nun als eigenständiger, ersatzfähiger Sachschaden.
- **Streichung des 500-€-Selbstbehalts:** Verbraucher müssen bei Sach- und Datenschäden keinen Eigenanteil mehr tragen; es wird ab dem ersten Cent gehaftet.
- **Wegfall der 85-Mio.-€-Obergrenze:** Die gesetzliche Haftungshöchstgrenze für Personenschäden wird komplett abgeschafft – die Haftung ist nun ungedeckt.

## Regierungsentwurf eines Gesetzes zur Modernisierung des Produkthaftungsrechts vom 17.12.2025

### 5. Neue Beweisregeln:

- **Pflicht zur Offenlegung von Beweismitteln:** Gerichte können Hersteller nun dazu verpflichten, interne Unterlagen, Sicherheitsdokumente oder Algorithmen-Codes offenzulegen, wenn der Kläger den Anspruch plausibel begründet (§ 19 Abs. 1).
- **Fehlervermutung bei Verweigerung:** Verweigert der Hersteller die gerichtliche Offenlegung dieser Beweismittel, wird rechtlich automatisch vermutet, dass das Produkt fehlerhaft war (§ 20 Abs. 1 Nr. 1).
- **Fehlervermutung bei Verstoß gegen Schutzpflichten:** Verstößt der Hersteller gegen verbindliche Sicherheits- oder regulatorische Vorgaben (wie z. B. vorgeschriebene Cybersicherheits-Updates), wird das Vorliegen eines Produktfehlers gesetzlich vermutet. (§ 20 Abs. 1 Nr. 2).
- **Fehlervermutung bei typischen Schäden:** Ein Produktfehler wird auch vermutet, wenn der Kläger nachweist, dass eine Rechtsgutverletzung durch eine offensichtliche Funktionsstörung des Produkts bei vernünftigerweise vorhersehbarem Gebrauch oder gewöhnlichen Umständen verursacht wurde (§ 20 Abs. 1 Nr. 3).
- **Erleichterung bei wissenschaftlicher/technischer Komplexität:** Es wird vom Fehler des Produkts ausgegangen, wenn der Kläger aufgrund der extremen Komplexität des Produkts (z. B. bei "Black-Box"-KI-Systemen) den Fehler oder die Kausalität nicht präzise nachweisen kann. Hierzu reicht es aus, wenn er die *Wahrscheinlichkeit* des Fehlers/Zusammenhangs mit dem Schaden nachweist (§ 20 Abs. 3).

## Regierungsentwurf eines Gesetzes zur Modernisierung des Produkthaftungsrechts vom 17.12.2025

### 6. Neues zum Haftungsausschluss:

- **Entwicklungsrisiko (§ 9 Abs. 1 Nr. 3):** Wenn der Fehler nach dem objektiven Stand von Wissenschaft und Technik zu dem maßgeblichen Beurteilungszeitpunkt (nach § 8) schlicht unmöglich erkannt werden konnte.
- **Rückausnahme für digitale/vernetzte Produkte (§ 9 Abs. 2 Satz 2):** Der Haftungsausschluss bei nachträglichen Fehlern gilt **nicht** (der Hersteller haftet also doch), wenn er die Kontrolle nach § 8 Abs. 2 behalten hat und der Fehler auf eines der folgenden vier Dinge zurückzuführen ist:
  - Einen mit dem Produkt verbundenen digitalen Dienst (§ 9 Abs. 2 Satz 2 Nr. 1).
  - Software, einschließlich nachträglicher Software-Updates oder -Upgrades (§ 9 Abs. 2 Satz 2 Nr. 2).
  - Das schuldhafte *Fehlen* von notwendigen Sicherheitsupdates, die zur Erhaltung der Produktsicherheit erforderlich gewesen wären (§ 9 Abs. 2 Satz 2 Nr. 3).
  - Eine nachträgliche wesentliche Änderung des Produkts (§ 9 Abs. 2 Satz 2 Nr. 4).
- **Schutz des Komponentenherstellers (§ 9 Abs. 3):** Wer nur ein Zulieferteil oder Softwareelement beisteuert, ist von der Haftung befreit, wenn der spätere Fehler des Gesamtprodukts allein auf das Design des Endprodukts oder auf falsche Anweisungen des Hauptherstellers zurückzuführen ist.
- **Schutz des Umgestalters / Upcyclers (§ 9 Abs. 4):** Wer ein Produkt wesentlich verändert und neu anbietet, haftet nicht für Fehler, die in Produktteilen liegen, die von seiner Änderung überhaupt nicht betroffen waren und unberührt geblieben sind.

## Regierungsentwurf eines Gesetzes zur Modernisierung des Produkthaftungsrechts vom 17.12.2025

- **Verjährung (§ 16):**
  - Der Anspruch auf Schadensersatz verjährt in **drei Jahren**. Die Verjährungsfrist beginnt mit dem Tag, an dem der Gläubiger von dem Fehler des Produkts, dem Schaden und der Identität des Schuldners Kenntnis erlangt hat oder hätte erlangen müssen. Im Übrigen sind die Vorschriften des Bürgerlichen Gesetzbuchs über die Verjährung anzuwenden. (§ 16).
  - Bei Verjährung bleibt ein Anspruch bestehen, kann aber nach Eintritt der Verjährung nicht mehr durchgesetzt werden, wenn durch den Hersteller die Einrede der Verjährung erhoben wird („Über Einreden muss man reden“).
- **Erlöschen (§ 17):**
  - Grundsätzlich erlischt der Anspruch auf Schadensersatz **10 Jahre** nachdem das fehlerhafte Produkt vom Hersteller in den Verkehr gebracht oder in Betrieb genommen wurde (*Abs. 1*).
  - Wird ein Produkt später **wesentlich verändert**, beginnt die 10-Jahres-Frist für dieses veränderte Produkt noch einmal ganz neu — und zwar ab dem Tag, an dem es nach der Änderung auf den Markt gebracht oder in Betrieb genommen wurde. (*Abs. 2*)
  - **Wenn es sich um eine Körper- oder Gesundheitsverletzung handelt, die eine lange Latenzzeit hat (also die Schäden erst sehr viel später auftreten), verlängert sich die Erlöschensfrist auf 25 Jahre. (Abs. 3)**
  - Beim **Erlöschen** geht der Anspruch auf Schadensersatz vollständig unter und existiert nicht mehr. Ein Gericht muss von Amts wegen prüfen, ob ein Anspruch erloschen ist.

## Verschuldensabhängige Produzentenhaftung nach § 823 Abs. 1 BGB

- Allgemeine Voraussetzungen:
  - Rechtsgutsverletzung (*Leben, Körper, Gesundheit, Freiheit, Eigentum oder ein sonstiges Recht [z.B. allgemeines Persönlichkeitsrecht oder Recht am eingerichteten oder ausgeübten Gewerbebetrieb]*) eines anderen
  - Verletzungshandlung
    - entweder Aktives Tun
    - oder Unterlassen
  - Kausalität zwischen der Verletzungshandlung und der Rechtsgutsverletzung
  - Rechtswidrigkeit
  - Verschulden (Vorsatz oder Fahrlässigkeit)
- Im Rahmen der Produzentenhaftung besteht der Vorwurf regelmäßig darin, dass der Hersteller schuldhaft ein fehlerhaftes Produkt in den Verkehr gebracht hat.
- Konkret: Verstoß des Herstellers gegen die sog. Verkehrssicherungspflichten.
  - Danach ist derjenige, der eine Gefahrenlage oder -quelle gleich welcher Art schafft und andauern lässt, verpflichtet, Rücksicht auf die Gefährdung zu nehmen und die zumutbaren Vorkehrungen zu treffen, um Schädigungen von Dritten möglichst zu verhindern.
  - Für die Produzentenhaftung haben sich diesbezüglich vier Fallgruppen mit speziellen Verpflichtungen herausgebildet (*siehe nächste Folie*).

## Spezielle Pflichten im Rahmen der Produzentenhaftung (allg. dargestellt)

Grds. sind Hersteller i.S. der Produzentenhaftung dazu verpflichtet, alle objektiv erforderlichen und zumutbaren Maßnahmen zu treffen, um andere vor Schäden zu bewahren, die durch die in Verkehr gebrachten Produkte entstehen.

- |                                 |                                                                                                                                                                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Organisationspflichten       | Der Hersteller hat seinen Betrieb so einzurichten, dass Fehler im Rahmen der Produktion (Fabrikation), Konstruktion und Instruktion möglichst ausgeschaltet oder durch Kontrollen entdeckt werden.                                                                 |
| 2. Instruktionspflichten        | Der Hersteller hat Hinweis- und Warnpflichten, etwa dahingehend, wie mit dem Produkt zur Schadensvermeidung umzugehen ist.                                                                                                                                         |
| 3. Produktbeobachtungspflichten | Wird nach Inverkehrbringen festgestellt, dass von dem Produkt eine Gefahr ausgeht, so hat der Hersteller diese Gefahren im Rahmen des ihm Zumutbaren abzuwenden. Umfasst davon sind die bereits in Verkehr gebrachten Produkte als auch die zukünftige Produktion. |
| 4. Gefahrabwendungspflichten    | Nach Bekanntwerden von drohenden Gefahren durch das Produkt, muss der Hersteller für die Vermeidung sorgen.                                                                                                                                                        |

## Spezielle Anforderungen und Pflichten für Wirtschaftsakteure bzgl. Hochrisiko-KI-Systemen nach der KI-VO

### 1. Pflichten für Anbieter

- Einrichtung eines Risikomanagementsystems (Art. 9)
- Strikte Daten-Governance (Art. 10)
- Erstellung der Technischen Dokumentation (Art. 11)
- Automatische Protokollierung (Art. 12)
- Transparenz und Bereitstellung von Informationen (Art. 13)
- Gewährleistung menschlicher Aufsicht (Art. 14)
- Genauigkeit, Robustheit und Cybersicherheit (Art. 15)
- Qualitätsmanagementsystem (Art. 17)
- Konformitätsbewertung, Konformitätserklärung und CE-Kennzeichnung (Art. 43, 47, 48)
- Registrierung in der EU-Datenbank (Art. 49)
- Meldung schwerwiegender Vorfälle (Art. 73)

### 2. Pflichten für Einführer (Importeure) und Händler

- Prüfpflicht vor Marktbereitstellung (Art. 23 & Art. 24)
- Rollenwechsel zum Anbieter (Art. 25)

## Was noch zum Thema Produzentenhaftung?

- Allein die Einhaltung nachrangiger harmonisierter (ISO-) Normen beim Qualitätsmanagement führt nicht zu einer Haftungsbefreiung von MP-Herstellern bzw. KI-Anbietern!
- In Bezug auf das nach § 823 Abs. 1 BGB erforderliche Verschulden kehrt die Rechtsprechung die Beweislast zugunsten des Geschädigten um und bemüht im Übrigen bei typischen Kausalverläufen häufig die Grundsätze über den Anscheinsbeweis.
- Fraglich ist, ob die in dem verworfenen Entwurf der KI-Haftungsrichtlinie berücksichtigten Beweislastfragen (z.B. bzgl. „Blackbox“) vom europäischen Gesetzgeber zukünftig nochmal in Angriff genommen werden, ebenso wie die Beweiserleichterungen und/oder Offenlegungspflichten der KI-Anbieter zugunsten der Geschädigten.

## Zivilrechtliche Haftung aufgrund Verletzung eines Schutzgesetzes i.S. des § 823 Abs. 2 BGB

- Ein weiterer Typus der verschuldensabhängigen Haftung stützt sich auf die Verletzung von Schutzgesetzen. In Betracht hierfür kommen hinsichtlich KI-basierten Medizinprodukten bzw. Medizinprodukten mit KI-Komponenten
  - MDR-Vorschriften, die den Patienten- und Gesundheitsschutz gewährleisten sollen (z.B. zu *Inverkehrbringen und Inbetriebnahme i.S. des Art. 5*);
  - § 12 Nr. 1 Medizinproduktedurchführungsgesetz (*Verbot des Inverkehrbringens von Produkten bereits im Fall eines Fehlerverdachts*);
  - Die besonderen Vorgaben bzgl. Hochrisiko-KI (*Art. 8-27 und 50 KI-VO*).

## Betreiberhaftung/Besondere Anforderungen an Betreiber von Hoch-Risiko-KI

- **Verschuldenshaftung (§ 823 Abs. 1 BGB)** Haftung bei Verletzung von Leben, Körper, Gesundheit oder Eigentum durch fahrlässigen oder vorsätzlichen Fehlgebrauch der KI.
- **Haftung für Verrichtungsgehilfen (§ 831 BGB)** Haftung des Betreibers für Schäden, die Mitarbeiter durch den Einsatz von KI verursachen (Exkulpationsmöglichkeit bei Sorgfaltsnachweis).
- **Vertragliche Haftung (§ 280 BGB)** Schadensersatz bei Pflichtverletzungen aus bestehenden Verträgen (z. B. Fehlberatung durch einen KI-Chatbot).
- **Art. 26 KI-VO (Pflichten der Betreiber von Hochrisiko-KI-Systemen):**
  - Sicherstellung geeignete KI-Nutzung nach Betriebsanleitung (Abs. 1)
  - Garantie Menschliche Aufsicht (Abs. 2)
  - Sorge für Qualität der Eingabedaten (Abs. 4)
  - Kontinuierliche Überwachung & Meldepflichten (Abs. 5)
  - Automatische Protokollierung (Logs, Abs. 6)
  - Unterstützung DSB bei der Datenschutz-Folgenabschätzung (Abs. 9)
- **Mögliche Sanktionen bei Nichteinhaltung der KI-VO-Anforderung:**
  - Geldbuße (Art. 99 KI-VO)
  - Behördliche Nutzungsuntersagung (Art. 79 Abs. 5 KI-VO)

## Betreiberhaftung/Besonderheiten Arzthaftung in Zusammenhang mit KI

- Eine KI ist nicht „Dr. Algorithmus“, es bleibt bzgl. ärztlicher Kerntätigkeiten bei den Grundsätzen des Arztvorbehalts und der persönlichen Leistungserbringung.
  - Problem: Labor-/radiologische Diagnosesysteme: Persönliche Überprüfung der technischen KI-Analyse immer möglich?
- Ärzte, die berufsmäßig KI verwenden, sind „Betreiber“ i.S. des Art. 2 Nr. 4 KI-VO.
- Die KI-VO beinhaltet keine eigenen Regeln zur Betreiber-Haftung. Grundsätzlich gelten deswegen beim medizinischen Einsatz von KI und daraus resultierenden Schäden die „normalen“ Prinzipien der Arzthaftung!
- Noch sind keine originär medizinrechtlichen Urteile zur KI-Betreiberhaftung bekannt, aber zu anderen Sachverhalten:
  - **LG Kiel:** Ein Unternehmen kann sich beim bewussten Einsatz einer KI zur Beantwortung von Suchanfragen nicht darauf berufen, nicht an dem automatisierten Verfahren beteiligt gewesen zu sein. Vielmehr habe sich im konkreten Fall das Unternehmen die KI-generierten Inhalte zu eigen gemacht und nach außen erkennbar die inhaltliche Verantwortung übernommen. Deswegen hafte das Unternehmen für die durch die KI verursachte Falschinformationen als sog. „Störer“ (vgl. Urteil vom 29.2.2024 - 6 O 151/23).
  - **LG Hamburg:** „An der äußerungsrechtlichen Unzulässigkeit der Darstellung ändert sich auch nicht deshalb etwas, weil der ehrbeeinträchtigende Beitrag KI-generiert ist. Insoweit macht sich der Betreiber des Accounts den Inhalt zu eigenen und hat für diese einzustehen“ (vgl. Beschluss vom 23.9.2025 - 324 O 461/25).
  - **Kammergericht Berlin:** Das KG klar, dass Rechtsanwälte für KI-generierte Inhalte voll haften. Die Pflicht zur gewissenhaften Berufsausübung erfordert eine strikte Letztkontrolle aller durch KI erzeugten Zitate und Fundstellen (vgl. Beschluss vom 20.11.2025, Az. 11 WF 144/25).

## Abschlussquiz zum Haftungsrecht



**Noch Fragen?**

## **RAin Walburga van Hövell, LL.M. (Medizinrecht)**

Dr. Fandrich Rechtsanwälte  
Partnerschaftsgesellschaft mbB  
Alexanderhaus  
Alexanderstraße 10  
53111 Bonn

**T** +49 228 / 41 00 28 70

**F** +49 228 / 41 00 28 79

**E** [whoevell@fandrich-rae.de](mailto:whoevell@fandrich-rae.de)

**W** [www.dr-fandrich-rechtsanwaelte.de](http://www.dr-fandrich-rechtsanwaelte.de)