Whitepaper

SKW Schwarz

Digital Health

Das Zusammenspiel von Regulatorik, KI und Datenschutz in der Medizintechnik – 20 Fragen und Antworten

Stand September 2024

Digital Health

Das Zusammenspiel von Regulatorik, KI und Datenschutz in der Medizintechnik – 20 Fragen und Antworten

1. **Warum ist das Zusammenspiel von Regulatorik, KI und Datenschutz entscheidend für die moderne Medizintechnik?**
2. **Was wären denkbare Anwendungsfälle in der Praxis?**
3. **Wann ist ein Medizinprodukt bzw. ein In-Vitro-Diagnostikum ein „KI-System“ im Sinne des AI Act, bzw. wann enthält es ein „KI-System“?**
4. **Welche Arten von KI, die der AI Act unterscheidet, sind für Medizintechnik besonders relevant?**
5. **Wie sind Medizinprodukte und IVD, die KI-Systeme enthalten, in diese Risikoklassen einzuordnen?**
6. **Welche regulatorischen Anforderungen gelten nach dem AI Act für Medizinprodukte/IVD mit KI-Systemen?**
7. **Welche Gemeinsamkeiten haben die KI-Regulatorik und die MDR/IVDR-Regulatorik?**
8. **Wie ist das Verhältnis zwischen AI Act und MDR/IVDR?**
9. **Welche Probleme bestehen aktuell bei der CE-Zertifizierung von Medizinprodukten und In-Vitro-Diagnostika mit KI unter der MDR/IVDR? Kann der AI Act diese lösen?**
10. **Steht der Datenschutz dem Einsatz von Medizinprodukten mit Künstlicher Intelligenz entgegen?**
11. **Wer muss die datenschutzrechtliche Anforderungen der DS-GVO umsetzen?**
12. **Wie können Medizinprodukte mit KI datenschutzkonform eingesetzt werden?**
13. **Wie kann eine KI mit Gesundheitsdaten datenschutzkonform trainiert werden?**
14. **Welche Datensätze dürfen zum Trainieren einer KI überhaupt verwendet werden?**
15. **Wann sind Gesundheitsdaten anonymisiert und wann pseudonymisiert?**
16. **Dürfen Datensätze des Medizinprodukts an Dritte weitergegeben werden?**
17. **Müssen Hersteller und Anwender von Medizinprodukten, die KI beinhalten, eine Datenschutz-Folgenabschätzung durchführen?**
18. **Welche Anforderungen gelten in Bezug auf die Datensicherheit?**
19. **Welche Anforderungen gelten in Bezug auf die Transparenz?**
20. **Was heißt das alles für die praktische Herangehensweise von Medizinprodukteanbietern, die KI-Systeme einsetzen wollen?**

Inhalt

Teil I: Themenaufriss und Darstellung der Use Cases

1. Warum ist das Zusammenspiel von Regulatorik, KI und Datenschutz entscheidend für die moderne Medizintechnik?

→ Der Einsatz von Künstlicher Intelligenz (KI) im Gesundheitswesen revolutioniert die medizinische Forschung, Entwicklung und Versorgung im Eiltempo. Fachkräftemangel, Effizienzdruck und der Ruf nach immer schnellerer und besserer Diagnostik und Therapie zwingen zur Digitalisierung und Unterstützung der menschlichen Arbeit durch leistungsfähige Technik. Beispielsweise kann KI-basierte Auswertungssoftware für bildgebende Diagnoseverfahren genutzt werden, um eine dann vom Arzt oder der Ärztin zu prüfende Erstdiagnose zu stellen. KI-Systeme werden zudem künftig anhand von Gesundheitsdaten sich anbahnende oder in der Entwicklung befindliche Krankheiten noch früher erkennen können.

KI führt in der Medizin zu völlig neuen Methoden und Möglichkeiten. Allerdings dürfen die Risiken nicht übersehen werden. Im Gesundheitswesen eingesetzte KI-Systeme müssen sicher, zuverlässig und leistungsfähig sein. Nur so entsteht Vertrauen in die neue Technik. Deshalb bedarf es hier auch neuer rechtlicher und regulatorischer Vorgaben und Absicherungsmechanismen.

Da KI große Mengen von Daten benötigt, um trainiert zu werden und sich so stetig zu verbessern, spielt beim Einsatz von KI in der Medizin auch der Datenschutz eine wichtige Rolle. Dies gilt umso mehr, als es sich bei den Gesundheitsdaten der Patienten um sehr sensible Informationen handelt, die in besonderem Maße geschützt werden.

Die Einhaltung der rechtlichen Vorgaben der Medizinprodukte- und In-Vitro-Diagnostika-Regulatorik, der neuen KI-Verordnung der EU (nachstehend „AI Act“ genannt) und der Anforderungen des Datenschutzes sind somit nicht nur notwendige Compliance-Aufgaben jedes Unternehmens, jedes Krankenhauses und jeder Arztpraxis. Sie sind nichts weniger als die Grundlage für den wirtschaftlichen und medizinischen Erfolg der neuen KI-basierten Technologien.

Der Einfluss des AI Act auf die täglichen Aufgaben der Medizintechnik-Unternehmen in der Regulatorik und in Bezug auf den rechtskonformen Umgang mit Daten führt zu neuen Rechtsproblemen und vielen offenen Fragen. Auch die Anwender – v.a. Krankenhäuser und Arztpraxen – müssen für einen rechtssicheren Einsatz der neuen KI-Technik sorgen. Mit diesem Whitepaper beleuchten wir deshalb für Sie das Zusammenspiel der neuen Regelungen im „magischen Dreieck“ Regulatorik – KI – Datenschutz und beantworten die wichtigsten Fragen zu diesen neuen Themen.

2. Was wären denkbare Anwendungsfälle in der Praxis?

→ Doch was bedeutet dies nun in der Praxis? Wie könnte sich das Verhältnis zwischen Regulatorik, KI und Datenschutz konkret auswirken? Um dies jeweils praxisnah zu illustrieren, stellen wir Ihnen zwei fiktive, aber realitätsnahe KI-Medizinprodukte als mögliche „Use Cases“ vor. Anhand dieser beiden fiktiven Produkte werden wir zu den Fragen und Antworten im Whitepaper jeweils verdeutlichen, was die dargestellten Rechtsprinzipien konkret für den Umgang mit neuer KI-Medizintechnik bedeuten.

1. Fall: Das Blutdruck-Messgerät „Blusser“

Das erste fiktive Beispielprodukt ist „Blusser“, ein Blutdruck-Messgerät. Dieses enthält eine KI-Software, die in einem Medizinprodukt eingebettet ist (sogenannte „embedded software“). „Blusser“ wird von den Patienten zu Hause angewendet. Die Software wertet die gemessenen Blutdruck-Werte sowie deren Verlauf aus und schließt daraus auf mögliche pathologische Zustände. Wird ein solcher erkannt, so weist die Software den Patienten bzw. die Patientin darauf hin und fordert dazu auf, sich ärztlich untersuchen zu lassen. Auf diese Weise betreibt die im Blutdruck-Messgerät integrierte KI eine präventive Diagnostik. Der Hersteller verbessert die KI durch Training stetig und erstellt regelmäßig Updates für die Software. Diese können die Patienten dann über Wifi und das Heimnetzwerk selbständig downloaden und auf dem Gerät installieren.

2. Fall: Die Software „NeoplasKI“

Das zweite Beispielprodukt ist die fiktive Software „NeoplasKI“. Sie wird in der Krebsdiagnostik eingesetzt. NeoplasKI ist eine Standalone-Software, also ein eigenständiges Produkt, das ohne Hardware ausgeliefert wird. Sie kann auf jedem PC installiert werden und enthält ein dynamisches KI-System. NeoplasKI ist dazu bestimmt, eine eigenständige Erstdiagnose zu erstellen, um so Radiologen in ihrer Arbeit zu entlasten. Dafür analysiert die Software Bildgebungen aus der Mammografie und berücksichtigt dabei auch die Entwicklung des Verlaufs, indem sie frühere Bildgebungen mit aktuellen vergleicht. Die von NeoplasKI durchgeführte Erstdiagnose wird dann von einem Radiologen bzw. einer Radiologin überprüft und verifiziert. Entweder wird das Ergebnis der Software dann von diesem bzw. dieser bestätigt oder – falls der Befund von NeoplasKI unzutreffend ist – abgeändert.

NeoplasKI wird zudem durch die ausgewerteten Bildgebungen und die ärztlichen Überprüfungen und Bewertung der von der KI erstellten Erstdiagnose fortlaufend verbessert und lernt hierdurch stetig dazu.

Teil II:
MDR-/IVDR-Regulatorik und KI

3. Wann ist ein Medizinprodukt bzw. ein In-Vitro-Diagnostikum ein „KI-System“ im Sinne des AI Act, bzw. wann enthält es ein „KI-System“?

→ Gemäß Art. 3 Abs. 1 AI Act ist ein „KI-System“ ein maschinengestütztes System,

- das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie betrieben werden kann,
- das nach der Einführung Anpassungsfähigkeit zeigen kann und
- das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen können.

KI-Systeme sind **softwarebasierte Systeme**. Folglich fallen Medizinprodukte und In-Vitro-Diagnostika (IVD), die bestimmungsgemäß ohne Software betrieben werden, von vornherein nicht unter die Definition eines „KI-Systems“ und damit auch nicht unter den AI Act.

Umgekehrt unterliegen Medizinprodukte und IVD mit Software nicht automatisch dem AI Act. Durch die Definition in Art. 3 Abs. 1 AI Act soll eine Abgrenzung von herkömmlichen Softwaresystemen oder Programmieransätzen vorgenommen werden, die auf den ausschließlich von natürlichen Personen festgelegten Regelung zur automatischen Ausführung von Vorgängen beruhen. Von solcher „einfacher“ Software unterscheidet sich ein KI-System im Kern dadurch, dass das KI-System nicht nur vorgegebene Programmabläufe (z.B. einprogrammierte Wenn-Dann-Verknüpfungen) abarbeitet, sondern darüber hinaus **über die Fähigkeit verfügt, zu lernen, eigene Schlussfolgerungen zu ziehen oder Modellierungen autonom vorzunehmen** (vgl. Erwägungsgrund 12 des AI Act).

Ein Medizinprodukt bzw. IVD kann bereits ein **eigenständiges KI-System** sein. KI-Systeme können aber auch Bestandteile von Medizinprodukten bzw. IVD neben anderen Komponenten sein, entweder ohne feste Integration oder als **integriertes, eingebettetes System**.

Praktische Anwendung auf die Beispielsfälle: Das Beispielprodukt „NeoplasKI“ ist eine KI-gestützte Diagnosesoftware und so als eigenständiges KI-System ein Medizinprodukt. Das KI-System in „Blusser“ hingegen ist ein Bestandteil eines Medizinprodukts. „Blusser“ enthält eine KI-gestützte Auswertungssoftware, die in einem Messgerät für bestimmte Vitalparameter integriert ist.

4. Welche Arten von KI, die der AI Act unterscheidet, sind für Medizintechnik besonders relevant?

→ Der AI Act sieht eine Klassifizierung von KI-Systemen nach Risikoklassen vor (ähnlich dem Medizinprodukterecht). Folgende Risikogruppen unterscheidet die Verordnung:

- Unannehmbares Risiko → **verbotene** KI-Praktiken (Art. 5 AI Act)
- Hochrisiko-KI-Systeme → **regulierte** KI-Systeme mit hohem Risiko (Art. 6-49 AI Act)
- KI-Systeme mit begrenztem Risiko → lediglich primär **Informationspflichten** (Art. 50 AI Act)
- KI-Systeme mit geringem oder ohne Risiko → **keine Verpflichtungen**, nur freiwillige Selbstregulierung (Erwägungsgrund 165 iVm Art. 95 AI Act)

5. Wie sind Medizinprodukte und IVD, die KI-Systeme enthalten, in diese Risikoklassen einzuordnen?

→ Nach dem Risikoklassifizierungssystem des AI Act sind Medizinprodukte und IVD, die KI-Systeme sind oder KI-Systeme enthalten (vgl. Frage 3), **oft Hochrisiko-KI-Systeme**. Dies ergibt sich aus Art. 6 Abs. 1 des AI Act. Demnach gilt ein Medizinprodukt als Hochrisiko-KI-System, wenn die beiden folgenden Bedingungen kumulativ erfüllt sind:

- **Erste Bedingung:** Das KI-System ist zur Verwendung als Sicherheitsbauteil eines Produkts bestimmt oder das KI-System ist selbst ein Produkt, das unter die in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union fällt. Gemäß Anhang I, Abschnitt A, Nr. 11 und 12 sind die MDR und die IVDR solche Harmonisierungsrechtsvorschriften. Wenn also das Medizinprodukt bzw. IVD sich im KI-System erschöpft (Beispiel: Diagnosesoftware), dann ist die erste Bedingung für ein Hochrisiko-KI-System erfüllt. Gleiches gilt, wenn das KI-System als eingebettetes oder nicht eingebettetes Teilsystem in einem Medizinprodukt bzw. IVD dort sicherheitsrelevante Aufgaben übernimmt und deshalb als „Sicherheitsbauteil“ eines Medizinprodukts bzw. IVD anzusehen ist (Art. 6 Abs. 1 lit. a)).

- **Zweite Bedingung:** Das Produkt, dessen Sicherheitsbauteil das KI-System ist, oder das KI-System selbst als Produkt muss einer Konformitätsbewertung durch einen Dritten unterzogen werden, damit dieses Produkt gemäß den in Anhang I aufgeführten Harmonisierungsrechtsvorschriften in Verkehr gebracht oder in Betrieb genommen werden kann. **Letzteres ist bei Medizinprodukten ab den Klassen Is, Im und Ir sowie bei IVD ab der Klasse B der Fall**; nur bei Medizinprodukten der Klasse I (außer Is, Im und Ir) und IVD der Klasse A genügt es für das Konformitätsbewertungsverfahren, wenn der Hersteller selbst die Konformität bewertet, sodass keine Konformitätsbewertung „durch einen Dritten“ erfolgen muss. Standalone-Software, die als Medizinprodukt zu qualifizieren ist, fällt allerdings nach den neuen Klassifizierungsregeln praktisch nie in die Klasse I, sondern fast immer in höhere Klassen, sodass bei solcher Software eingesetzte KI-Systeme regelmäßig Hochrisiko-KI-Systeme sind.

→ Im Umkehrschluss sind KI-Systeme dann **keine Hochrisiko-Systeme** nach diesen Vorschriften, wenn sie

- nur ein Bestandteil (eingebettet oder nicht integriert) eines Medizinprodukts bzw. IVD und damit nicht selbst das Produkt sind und kein Sicherheitsbauteil des Medizinprodukts/IVD sind, d.h. keine sicherheitsrelevante Funktion übernehmen (Bedingung 1 nicht erfüllt), **oder**

- das Medizinprodukt ein solches der Klasse I (ausgenommen Klassen Is, Im und Ir) bzw. das IVD ein solches der Klasse A ist (Bedingung 2 nicht erfüllt).

In der Praxis dürfte die erstgenannte Ausnahme jedoch kaum eingreifen. Aus Gründen der Patientensicherheit wird man den Begriff „Sicherheitsbauteil“ weit auslegen müssen. Gemäß Art. 3 Abs. 14 AI Act ist ein Sicherheitsbauteil eines Produkts oder Systems ein Bauteil eines Produkts oder eines Systems, das eine Sicherheitsfunktion für dieses Produkt oder System erfüllt oder dessen Ausfall oder Fehlfunktion die Gesundheit und Sicherheit von Personen oder Sachen gefährdet. In der Folge wird u.E. jede KI, die zumindest auch Auswirkungen auf die Sicherheit des Medizinprodukts/IVD hat, unter diesen Begriff fallen und somit zur Einstufung des KI-Systems als Hochrisiko-KI-System führen.

Im Anhang I finden Sie ein Prüfschema zur Einstufung von KI in Medizinprodukten und IVD.

Praktische Anwendung auf die Beispielsfälle: „Blusser“ sowie „NeoplasKI“ sind jeweils als Hochrisiko-Systeme im Sinne des AI Act einzustufen.

„Blusser“ ist als Blutdruck-Messgerät der Klasse IIa zuzuordnen und macht deshalb eine Konformitätsbewertung durch einen Dritten erforderlich. Das KI-System ist in dem Messgerät eingebettet und übernimmt dort sicherheitsrelevante Aufgaben. Es soll nämlich Blutdruckwerte auswerten und so pathologische Zustände erkennen, was der Sicherheit des Patienten dient. Eine Fehlfunktion könnte zu einer Gesundheitsgefährdung des Patienten führen, wenn dieser auf die Angaben des „Blussers“ vertraut. Die KI-Software im „Blusser“ ist somit unseres Erachtens als „Sicherheitsbauteil“ einzustufen. Beide Bedingungen einer Hochrisiko-KI sind erfüllt.

„NeoplasKI“ ist eine KI-gestützte Diagnosesoftware. Dieses Medizinprodukt erschöpft sich im KI-System selbst und fällt in den Anwendungsbereich der MDR, einer in Anhang I des AI Act aufgeführten Harmonisierungsrechtsvorschrift. Als Standalone-Software unterfällt „NeoplasKI“ nicht mehr der Klasse I der MDR und muss deshalb einer Konformitätsbewertung durch einen Dritten unterzogen werden; es reicht nicht aus, wenn der Hersteller selbst eine solche vornimmt. Auch hier sind beide Bedingungen einer Hochrisiko-KI nach Art. 6 des AI Act erfüllt.

6. Welche regulatorischen Anforderungen gelten nach dem AI Act für Medizinprodukte/IVD mit KI-Systemen?

→ Für Hochrisiko-KI-Systeme muss vor dem Inverkehrbringen ein Konformitätsbewertungsverfahren mit Prüfung, Bewertung und Ausstellung einer Konformitätsbescheinigung in Bezug auf die Standards und Anforderungen des AI Act durchgeführt werden.

Liegt ein Hochrisiko-KI-System vor – was bei Medizinprodukten und IVD mit KI meistens der Fall sein wird (siehe Frage 5) – so müssen gemäß dem Kapitel III des AI Act vor allem die folgenden Anforderungen zusätzlich zu den Anforderungen der MDR bzw. IVDR eingehalten werden:

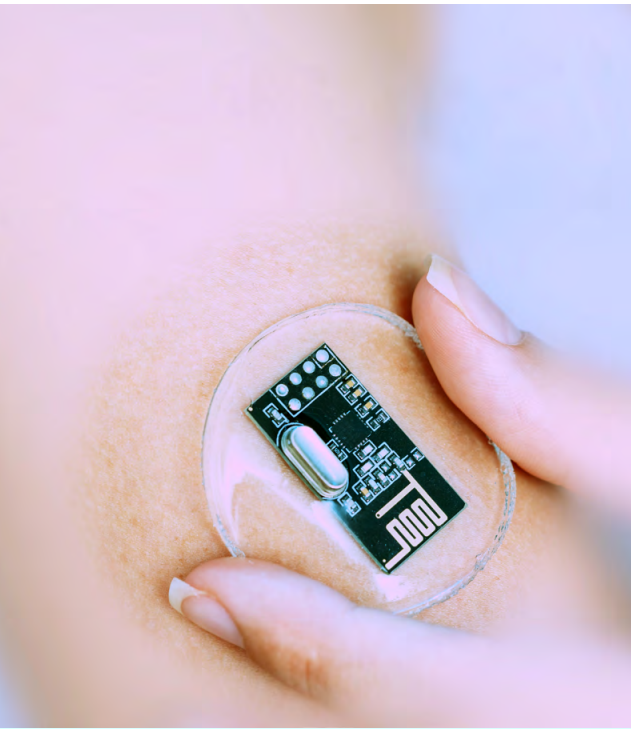
- Ein **Risikomanagementsystem** ist während des gesamten Lebenszyklus des KI-Systems einzurichten, umzusetzen, zu dokumentieren und aufrechtzuerhalten. Das Prinzip ähnelt methodisch und strukturell dem von der MDR bzw. IVDR geforderten Risikomanagementsystem, allerdings mit besonderer Berücksichtigung der KI-Spezifika (Art. 9 AI Act).

- **Hohe Anforderungen an die Qualität der Daten**, mit denen das Modell trainiert wird, insb. durch geeignete Datenverwaltungs- und Datenmanagementpraktiken (Art. 10 AI Act).

- Eine **Technische Dokumentation (TD)** muss vor dem Inverkehrbringen erstellt und stets auf dem neuesten Stand gehalten werden. Insoweit muss die für Medizinprodukte und IVD ohnehin benötigte TD um einige KI-spezifische Anforderungen ergänzt werden (Art. 11 AI Act).

- Technische Ermöglichung der **automatischen Aufzeichnung von Ereignissen** (Art. 12 AI Act).

- Erfüllung von **Transparenz- und angemessenen Informationspflichten** gegenüber den Anwendern (Art. 13 AI Act).



- Das Hochrisiko-KI-System muss so konzipiert und entwickelt werden, dass für die Dauer der Nutzung eine **menschliche, wirksame Beaufsichtigung gewährleistet** ist (Art. 14 AI Act).

- Einhaltung eines angemessenen Maßes an **Genauigkeit, Robustheit und Cybersicherheit** (Art. 15 AI Act).

- Anbieter von Hochrisiko-KI-Systemen müssen außerdem über ein **Qualitätsmanagementsystem nach Art. 17 AI Act** verfügen. Dieses entspricht allerdings weitestgehend dem QM-System nach ISO 13485 und der MDR/IVDR und ist somit für Hersteller von Medizinprodukten und IVD methodisch und strukturell nichts wesentlich Neues.

- Die **Bevollmächtigten**, die es nach Art. 22 AI Act geben muss, haben im Prinzip die gleichen Pflichten, die auch in der MDR/IVDR festgelegt werden.

7. Welche Gemeinsamkeiten haben die KI-Regulatorik und die MDR/IVDR-Regulatorik?

→ Insgesamt fällt auf, dass sich die KI-Regulatorik methodisch sehr stark an die Medizinprodukte- und IVD-Regulatorik anlehnt. Für Medizinprodukte-Unternehmen ist dies aus unserer Sicht Chance und Risiko zugleich. Einerseits müssen hier zwar für Medizinprodukte mit KI-Systemen zusätzliche regulatorische Anforderungen erfüllt werden, was mit höherem Aufwand und damit höheren Kosten verbunden ist. Andererseits sind die Grundstrukturen für die Zusatzanforderungen (z.B. Risikomanagementsystem, Technische Dokumentation, Qualitätsmanagement nach ISO 13485) in aller Regel bereits vorhanden und für Unternehmen der MedTech-Branche – anders als z.T. für andere Branchen, die KI-Systeme verwenden wollen – auch nicht neu. Vorteilhaft ist, dass durch die Vorgaben des AI Act sehr viel klarer und deutlicher wird, welche Anforderungen konkret an ein Medizinprodukt mit KI-System gestellt werden und was dafür erfüllt und dokumentiert werden muss, damit eine Zertifizierung erfolgen kann.

8. Wie ist das Verhältnis zwischen AI Act und MDR/IVDR?

→ Das Verhältnis zwischen AI Act und MDR bzw. IVDR ist noch nicht vollständig geklärt. In Anhang I, Abschnitt A des AI Acts sind allerdings in Nr. 11 die Verordnung (EU) 2017/745 (MDR) und in Nr. 12 die Verordnung (EU) 2017/746 (IVDR) explizit als harmonisierte Normen angeführt. Das bedeutet in Bezug auf Medizinprodukte bzw. IVD mit KI-Systemen: Sind die Anforderungen der MDR oder IVDR bereits erfüllt (beispielsweise in Bezug auf das Risikomanagement, die technische Dokumentation, die entsprechende Konformitätsbewertung und Zertifizierung etc.), so gelten diese MDR-/IVDR-bezogenen Anforderungen auch im Rahmen des AI Act als erfüllt und müssen nicht mehr separat geprüft und nachgewiesen werden. Es müssen „nur noch“ die Anforderungen des AI Act an das KI-System des Medizinprodukts bzw. des IVD ergänzend eingehalten werden.

Aus Erwägungsgrund 124 und Art. 43 AI Act sowie dem Charakter der harmonisierten Normen ergibt sich dabei, dass immer nur ein Konformitätsbewertungsverfahren durchzuführen ist, in dem die Anforderungen aller relevanten Normen (AI Act und MDR bzw. IVDR) geprüft werden.

Konkret heißt das, dass Anbieter von Medizinprodukten mit KI-Systemen **beide Anforderungen einhalten** müssen, die der MDR und des AI Act, **aber nur ein einheitliches Konformitätsbewertungsverfahren durchführen** müssen. In diesem Verfahren werden beide Regelungsansätze berücksichtigt und das Medizinprodukt wird auf Konformität mit diesen Anforderungen geprüft und entsprechend zertifiziert. Entsprechendes gilt für IVD in Bezug auf die Anforderungen der IVDR und des AI Act.

9. Welche Probleme bestehen aktuell bei der CE-Zertifizierung von Medizinprodukten und In-Vitro-Diagnostika mit KI unter der MDR/IVDR? Kann der AI Act diese lösen?

→ Medizinprodukte und IVD benötigen eine CE-Kennzeichnung, damit sie auf dem europäischen Markt in den Verkehr gebracht oder in Betrieb genommen werden können. Die CE-Kennzeichnung darf nur angebracht werden, wenn das Produkt die grundlegenden Sicherheits- und Leistungsanforderungen erfüllt. Dies wird durch ein Konformitätsbewertungsverfahren sichergestellt, wobei bei Medizinprodukten der höheren Risikoklassen (bei Medizinprodukten ab Klasse Is, Im und Ir, bei IVD ab Klasse B) die Einbindung einer Benannten Stelle in das Konformitätsbewertungsverfahren erforderlich ist.

Bisher sind Benannte Stellen oft sehr zurückhaltend, Medizinprodukte und IVD mit dynamischer KI zu zertifizieren, weil sich die KI durch Hinzulernen verändert und sich damit die Risikobewertung und das Nutzen-Risiko-Profil der Produkte stetig verändern kann. Ähnliche Probleme können bei sogenannter „Black Box KI" bestehen, bei der der Dateninput und/oder die Operationen für den Benutzer (und damit im Zweifel auch für die Benannte Stelle) nicht nachvollziehbar und überprüfbar sind. Da es ein Wesen der KI ist, autonom Ergebnisse zu erzielen und Schlussfolgerungen zu ziehen, bei denen der Weg dahin nicht durch Programmierung vorgegeben ist, wird KI in Medizinprodukten und IVD häufig „Black Box KI" in diesem Sinn sein, mit entsprechenden Problemen bei der klassischen, auf ein mehr oder weniger statisches Produkt bezogenen Konformitätsbewertung der Benannten Stellen.

Auch wenn dieses Problem weder in der MDR/IVDR noch im AI Act konkret thematisiert wird, könnte hier der AI Act tatsächlich Abhilfe schaffen. **Der AI Act enthält nun konkrete regulatorische Vorgaben zur Risikobewertung und Risikokontrolle auch dynamischer KI** (siehe oben Frage 6). Diese Mechanismen können nun eingesetzt werden, um genau diejenigen Spezifika von KI-Systemen in Medizinprodukten und IVD abzudecken, die sich allein mit den Mechanismen der MDR/IVDR bisher aus Sicht der Benannten Stellen nur schwer in den Griff bekommen ließen.

Wir gehen davon aus, dass die Koordinierungsgruppe Medizinprodukte (MDCG) bald schon Dokumente herausgeben wird, die für Medizinprodukte und IVD mit KI-Systemen verwendet werden können, um die Konformitätsbewertung sowohl nach MDR/IVDR als auch nach dem AI Act koordinieren und abbilden zu können. Dies sollte es dann auch erleichtern, die Benannten Stellen zu überzeugen, da dann (endlich) ein vereinheitlichter Prozess für Medizinprodukte und IVD mit KI vorliegt. Es empfiehlt sich dann – wie auch sonst – die Technische Dokumentation soweit wie möglich an diesen Dokumenten auszurichten.

Teil III: Datenschutz und KI

10. Steht der Datenschutz dem Einsatz von Medizinprodukten mit Künstlicher Intelligenz entgegen?

→ Die Antwort lautet klar: Nein.

Richtig ist, dass gerade beim Einsatz von Medizinprodukten – insbesondere in Kombination mit Komponenten Künstlicher Intelligenz (KI) – datenschutzrechtliche Besonderheiten beachtet werden müssen. Zum einen entspricht es dem einhelligen Meinungsbild der Datenschutzaufsichtsbehörden, dass der Einsatz von KI mit Risiken einhergeht (Stichwort: Fehlende Transparenz, sogenannter „Black Box"-Gedanke). Zum anderen ist die Systematik der DS-GVO so aufgebaut, dass die Verarbeitung von Gesundheitsdaten grundsätzlich verboten ist (vgl. Art. 9 Abs. 1 DS-GVO), es sei denn, es greift eine der in Art. 9 Abs. 2 DS-GVO aufgezählten – tendenziell restriktiven – Ausnahmen. Komplex wird es schon bei der Frage, welche Rechtsgrundlage die Verarbeitung von Gesundheitsdaten zum Trainieren der KI legitimieren kann. Ebenfalls komplex wird es, sofern eine KI-Komponente im späteren Live-Betrieb gegebenenfalls eigenständige Entscheidungen trifft und dadurch der Anwendungsbereich des Art. 22 Abs. 1 DS-GVO eröffnet wird.

Gerade die Kombination dieser Themen kann die einschlägigen Akteure vor einige Herausforderungen stellen. Gleichwohl – dies zeigt die Beratungspraxis – sind die Herausforderungen unter Beachtung der notwendigen Prüfschritte in der überwiegenden Zahl der Fälle gut zu bewältigen.

11. Wer muss die datenschutzrechtliche Anforderungen der DS-GVO umsetzen?

→ Wer die in der DS-GVO festgelegten Anforderungen zu erfüllen hat, hängt von der datenschutzrechtlichen Rollenverteilung ab. Während der AI Act für bestimmte Konstellationen klare Rollenverteilungen vorsieht und die MDR/IVDR überwiegend den Hersteller adressieren, kann die datenschutzrechtliche Verantwortlichkeit von Fall zu Fall stark variieren.

In Art. 4 Nr. 7 DS-GVO wird insoweit festgehalten, dass der Verantwortliche als primärer Adressat der datenschutzrechtlichen Pflichten über die Zwecke und Mittel der Datenverarbeitung bestimmt. Während die Trainingsphase eines KI-gestützten Medizinprodukts typischerweise im Verantwortungsbereich des Herstellers liegt, rückt während der Anwendungsphase – etwa bei der Behandlung eines Patienten – regelmäßig die Arztpraxis oder das Krankenhaus in die Rolle des Verantwortlichen. In der Anwendungsphase kann der Hersteller jedoch insbesondere die Rolle eines Auftragsverarbeiters im Sinne des Art. 28 DS-GVO einnehmen, beispielsweise sofern er personenbezogene Daten – etwa cloudbasiert und/oder durch Fernwartungsarbeiten – im Auftrag des Anwenders verarbeitet. Spannend wird es insbesondere dann, wenn der Auftragsverarbeiter Nutzungsdaten zu eigenen Zwecken verwendet, etwa um die KI fortlaufend weiter zu trainieren. In diesem Fall wird der klassische Rahmen der Auftragsverarbeitung „durchbrochen“ und der Hersteller nimmt – zumindest für gewisse Verarbeitungsvorgänge – erneut die Rolle eines Verantwortlichen an. Ob dies zu einer getrennten oder gemeinsamen Verantwortlichkeit der Akteure führt, ist in der juristischen Diskussion umstritten und muss daher sehr gründlich geprüft werden. Seitens der Datenschutzaufsichtsbehörden geht die Tendenz hin zu einer gemeinsamen Verantwortlichkeit.

Merken kann man sich jedoch bereits an dieser Stelle, dass keine der vorgenannten Aussagen „in Stein gemeißelt“ ist, sondern stets eine umfassende Prüfung im Einzelfall durchzuführen ist.

Praktische Anwendung auf die Beispielsfälle: Am Beispiel des Medizinprodukts „NeoplasKI“ wäre zunächst davon auszugehen, dass der Hersteller die Verantwortung für den Trainingsprozess trägt. Insbesondere die Auswahl der richtigen Trainingsdaten sowie deren rechtmäßige Verarbeitung wären daher vom Hersteller der Software „NeoplasKI“ sicherzustellen.

Während der sich hieran anschließenden Nutzungsphase von „NeoplasKI“ würden demgegenüber die das Medizinprodukt einsetzenden Arztpraxen oder Krankenhäuser die Rolle des Verantwortlichen einnehmen. Sollte der Hersteller von „NeoplasKI“ zu diesem Zeitpunkt jedoch einen weiteren Zugriff auf personenbezogene Daten erhalten – etwa zur Durchführung von Fernwartungsarbeiten –, wäre insoweit von einer Auftragsverarbeitung auszugehen. Da die während der Nutzungsphase verarbeiteten Daten jedoch auch zum weiteren „Trainieren“ von „NeoplasKI“ genutzt werden sollen, steht gleichsam eine (getrennte oder gemeinsame) Verantwortlichkeit des Herstellers im Raum, welche sich auf eben diesen Trainingsprozess bezieht. Mindestvoraussetzung ist es daher, dass sich alle Beteiligten ein klares Bild über die datenschutzrechtlichen Rollenverteilungen verschaffen und diese entsprechend vertraglich abbilden.

12. Wie können Medizinprodukte mit KI datenschutzkonform eingesetzt werden?

→ Trotz bestehender Besonderheiten handelt es sich (auch) bei dem Einsatz von Medizinprodukten mit KI-Komponenten zunächst einmal um eine gewöhnliche Verarbeitung personenbezogener Daten.

Dies bedeutet, dass die allgemeinen Grundsätze aus Art. 5 Abs. 1 DS-GVO beachtet und angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO umgesetzt werden müssen. Die DS-GVO ist ausdrücklich technologieneutral ausgestaltet, weshalb der bloße Einsatz von KI zunächst keine eigenen gesetzlichen Besonderheiten mit sich bringt. In der aufsichtsbehördlichen Praxis ist allerdings die Tendenz zu erkennen, dass gerade an den Einsatz von KI – insbesondere im sensiblen Bereich der Gesundheitsdaten – strengere Maßstäbe angelegt werden.

Was bedeutet dies für die Praxis? In einem ersten Schritt sollte sich das betroffene Unternehmen (etwa der Hersteller eines entsprechenden Medizinprodukts) überlegen, in welchen „Lebenszyklen" der KI die Verarbeitung personenbezogener Daten eine Rolle spielt. Regelmäßig wird – auch wenn in der Praxis natürlich Überschneidungen denkbar sind – zwischen verschiedenen Phasen der Entwicklung und des Einsatzes einer KI differenziert:

- Entwicklungsphase
- Trainings- und Testphase
- Validierungsphase
- Einsatzphase

Für jede Phase müssen – von der jeweils verantwortlichen Stelle – sämtliche datenschutzrechtlichen Anforderungen beachtet werden. In der Entwicklungsphase müssen insbesondere die Konzeption sowie die (künftigen) Datenverarbeitungsschritte bedacht werden. Bei der Trainings- und Testphase kommt es vor allem auf die Auswahl der jeweiligen Trainings- und Testdaten sowie gleichsam auf die Umsetzung des Datenminimierungsgrundsatzes (Art. 5 Abs. 1 lit. c) DS-GVO) an. In dieser Phase sollte insbesondere auch die Entscheidung getroffen (und dokumentiert) werden, in welchem Umfang anonymisierte oder zumindest pseudonymisierte Daten genutzt werden können. Beim späteren Einsatz einer „fertig" trainierten KI wird insbesondere die Transparenz der Datenverarbeitung entscheidend sein (Art. 5 Abs. 1 lit. a) DS-GVO).

In der Praxis bewährt hat sich der Entwurf einer KI-Guidance, welche die einzelnen Prüfschritte – aufgeteilt nach den relevanten Lebenszyklen – konkret definiert. Sind die jeweiligen Anforderungen erstmal formuliert, gilt anschließend das Check-Listen-Prinzip. Auf diese Weise gelingt insbesondere auch die Einhaltung der Rechenschaftspflicht gegenüber der Datenschutzaufsichtsbehörde (Art. 5 Abs. 2 DS-GVO).

Bei der Konzeption sollten weitere regulatorische Fragestellungen mitgedacht werden (vgl. hierzu Teil II dieses Whitepapers).

13. Wie kann eine KI mit Gesundheitsdaten datenschutzkonform trainiert werden?

→ Dreh- und Angelpunkt eines datenschutzkonformen Trainings einer KI sind die hierbei zum Einsatz kommenden Trainingsdaten. Woher stammen diese? Verfügen diese über eine hinreichende Qualität und können sogenannte Bias ausgeschlossen werden? Auch werden im Regelfall nicht die bloßen „Rohdaten" zum Trainieren einer KI genutzt, sondern diese werden umfassend aufbereitet (sogenannte Standardisierung), sodass alle eingesetzten Daten die gleichen Qualitätsmerkmale aufweisen.

Wird beispielsweise ein sogenanntes **überwachtes Lernen** – wie dies bei Künstlichen Neuronalen Netzen zur Bildklassifizieriung und -segmentierung häufig anzutreffen ist – durchgeführt, müssen die jeweiligen Daten zunächst gelabelt (auch „beschriftet" oder „annotiert") werden. Beim überwachten Lernen werden der KI solche Daten vorgesetzt, deren Ergebnis (also die Antwort auf die zu prüfende Aufgabe) bereits bekannt ist. Die KI „erlernt" sodann über ständige Wiederholung den Zusammenhang zwischen Input und den weiter erforderlichen Gewichtungen zum Lösen der Aufgabe. Auch dieser Arbeitsschritt sollte möglichst gründlich geprüft werden, sodass klare Vorgaben und Qualitätssicherungsprüfungen für die Annotation der Trainingsdaten existieren.

Schwierig gestaltet sich häufig die Frage, auf **welche datenschutzrechtliche Rechtsgrundlage** die Datenverarbeitung gestützt werden kann. Hierbei sind gleich mehrere „Kniffe" zu beachten, die der Verantwortliche im Vorfeld prüfen sollte:

(1) **Ist die Herkunft der Trainingsdaten bekannt und dürfen diese Daten überhaupt genutzt werden?** Wie bereits weiter oben angeführt, ist die Verarbeitung von Gesundheitsdaten gemäß Art. 9 Abs. 1 DS-GVO grundsätzlich verboten. Da im Anwendungsbereich des Art. 9 DS-GVO keine originäre Interessenabwägungsklausel (wie in Art. 6 Abs. 1 lit. f) DS-GVO) existiert, wird man sich häufig mit einer datenschutzrechtlichen Einwilligung auseinandersetzen müssen – mit den bekannten Problemen der Informiertheit, Freiwilligkeit und Zweckgebundenheit.

(2) Häufig wird daneben die Frage zu beantworten sein, ob eine sogenannte **Zweckänderung** im Sinne des Art. 6 Abs. 4 DS-GVO vorliegt. Wurden die jeweiligen Daten etwa ursprünglich zu gänzlich anderen Zwecken erhoben, ist die nunmehr zweckfremde Verarbeitung der Daten aus datenschutzrechtlicher Sicht gesondert zu legitimieren.

(3) Je nach Funktionsweise und Architektur einer KI kann zudem die Frage klärungsbedürftig sein, **ob die eingesetzten Trainingsdaten auch künftig – etwa im Live-Betrieb – weiter genutzt werden.** Nutzt die fertig trainierte KI also auch in deren Einsatzphase die ursprünglich (nur) zum Trainingsvorgang vorgesehenen Daten? Oder handelt es sich „nur" um einen fertig trainierten Algorithmus, welcher – nach aktuellem technischen Stand – keinen Rückschluss auf die jeweiligen Daten zulässt? Da im ersten Fall wiederum ein „neuer" Zweck der Datenverarbeitung vorliegt, müssen bereits in der Trainingsphase einige Entwicklungen und technische Fragestellungen für die Zukunft mitberücksichtigt werden.

14. Welche Datensätze dürfen zum Trainieren einer KI überhaupt verwendet werden?

→ Wie bei jeder Verarbeitung personenbezogener Daten hat die Auswahl der genutzten Daten stets anhand des konkret verfolgten Zwecks zu erfolgen. Dies bedeutet, dass – unter Beachtung des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c) DS-GVO) – (nur) solche personenbezogenen Daten verarbeitet werden dürfen, welche zur Zweckerreichung tatsächlich benötigt werden (**Zweckbindungsgrundsatz**, Art. 5 Abs. 1 lit. b) DS-GVO).

In diesem Zusammenhang sind folgende Punkte zu bedenken:

- In einem ersten Schritt sollte stets geprüft werden, ob gegebenenfalls mit **anonymisierten Datensätzen** trainiert werden kann oder von vornherein auf reine Maschinendaten oder synthetische Daten zurückgegriffen werden kann. In diesem Fall käme die DS-GVO nämlich erst gar nicht zur Anwendung, was den datenschutzrechtlichen „Königsweg“ darstellen würde.
- Ist eine Anonymisierung nicht gegeben, nicht möglich oder nicht zweckmäßig, sollte über eine **Pseudonymisierung** nachgedacht werden. Pseudonymisierte Daten sind zwar weiterhin personenbezogene Daten. Die Pseudonymisierung ist im Datenschutzrecht jedoch als eine effektive Maßnahme anerkannt, die zu Gunsten der betroffenen Personen erheblich risiko- und eingriffsminimierend wirkt. Sie ist deshalb geeignet, zu einer positiven, datenschutzrechtlichen Risikobewertung beizutragen.
- Ist auch eine Pseudonymisierung nicht gegeben, nicht möglich oder nicht zweckmäßig, ist zumindest der jeweilige Datensatz selbst auf **überflüssige Datenpunkte** zu untersuchen. Im Falle von bildgebenden medizinischen Daten (z.B. CT-Bildern) könnten beispielsweise diejenigen Metadaten im Bild entfernt werden, die Rückschlüsse auf das jeweilige Krankenhaus oder weitere Informationen zulassen.

Dies vorweggestellt bleibt dennoch häufig das Dilemma, dass zum Trainieren einer KI eine hinreichend große Datenmenge verarbeitet werden muss. Um Diskriminierungen oder sonstige Fehlentscheidungen auszuschließen, werden regelmäßig vielfältige Datensätze (im Hinblick auf Geschlecht, Alter, Herkunft, Ethnie, etc.) verarbeitet. Auch steigt die Qualität der eingesetzten KI häufig gerade mit der Anzahl der durchgeführten Trainingsdurchläufe. Dies zeigt, dass sich das Spannungsfeld zwischen einerseits dem Bedürfnis, mit Hilfe großer Datenmengen möglichst weitreichende Erkenntnisse zu erzielen, und andererseits der Verpflichtung zur Beachtung des Datenminimierungsgrundsatzes gemäß Art. 5 Abs. 1 lit. c), in vielen Fällen kaum ganz konfliktfrei auflösen lässt.

Durch eine **hinreichende Dokumentation in einer KI-Guidance** (siehe hierzu bereits weiter oben) können die tragenden Erwägungen zur Auswahl der entsprechenden Trainingsdaten jedoch dokumentiert und insoweit sowohl für eine (datenschutz-)aufsichtsbehördliche Prüfung als auch für eine Dokumentation gegenüber Kunden und Abnehmern nachvollziehbar gemacht werden. Hierdurch kann der Verantwortliche seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO nachkommen. Außerdem kann eine solche KI-Guidance dazu eingesetzt werden, im Rahmen der Technischen Dokumentation im Konformitätsbewertungsverfahren nach der MDR/IVDR und dem AI Act die Einhaltung der KI-bezogenen Anforderungen zu belegen (siehe Frage 6).

Apropos Anforderungen an die Trainingsdatensätze: Der AI Act enthält seinerseits eigene Anforderungen in Bezug auf die **“Daten-Governance”**. Gemäß Art. 10 Abs. 1 AI Act dürfen Hochrisiko-KI-Systeme (zu denen viele Medizinprodukte und IVD mit KI-Elementen zählen, s. bereits Teil II dieses Whitepapers) nur mit solchen Daten trainiert werden, die bestimmten, in Art. 10 Abs. 2 - 5 AI Act genannten Qualitätskriterien entsprechen. Beispielsweise müssen die **Trainings-, Validierungs- und Testdatensätze “relevant, repräsentativ, fehlerfrei und vollständig**” sein (Art. 10 Abs. 3 AI Act). Hier drängt sich eine Parallele zu den unterschiedlichen datenschutzrechtlichen Anforderungen und Grundsätzen in Art. 5 Abs. 1 DS-GVO auf. So müssen gemäß Art. 5 Abs. 1 lit. d) DS-GVO personenbezogene Daten (ebenfalls) “sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein” und “es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden”.

Dies zeigt: **Regulatorische Anforderungen aus dem AI Act bzw. der MDR/IVDR einerseits und datenschutzrechtliche Anforderungen gehen inhaltlich teilweise “Hand in Hand”**. Dennoch ist Zurückhaltung dahingehend geboten, die Anforderungen der unterschiedlichen Regelwerke miteinander “zu vermengen”. Dies gilt insbesondere für die Technische Dokumentation, die im Konformitätsbewertungsverfahren nach MDR/IVDR und nach Art. 11 AI Act erstellt werden muss. Diese sollte nicht unnötig mit den datenschutzrechtlich gebotenen Dokumentationen “angedickt” werden. Im Zweifel sollte man sich dort vielmehr an die Struktur- und Inhaltsvorgaben der MDCG-Dokumente halten. Umgekehrt dürfte jedoch die Technische Dokumentation gemäß der MDR/IVDR und dem AI Act gut im Rahmen der datenschutzrechtlichen Dokumentation nach Art. 5 Abs. 2 DS-GVO verwertbar sein.

15. Wann sind Gesundheitsdaten anonymisiert und wann pseudonymisiert?

→ Wie oben ausgeführt stellt die Anonymisierung den datenschutzrechtlichen „Königsweg“ dar. Daten sind personenbezogen, wenn sie sich auf eine natürliche Person beziehen und eine direkte (etwa über den Namen) oder zumindest indirekte Identifizierung der Person (etwa über eine Kennnummer) möglich ist.

Von einer **Anonymisierung** ist dann auszugehen, **wenn eine natürliche Person nicht (mehr) identifizierbar ist**. Sämtliche Klardaten oder sonst mittelbar identifizierbaren Merkmale müssen daher aus dem Datensatz entfernt werden. Eine **Pseudonymisierung** verfolgt demgegenüber den Zweck, die jeweilige Person – etwa unter Vergabe einer Patienten-ID bei Klinischen Studien – **im Anschluss wieder identifizieren zu können**. Bei pseudonymisierten Daten handelt es sich daher weiterhin – da eine Zuordnung etwa über die vergebene Patienten-ID möglich bleibt – um personenbezogene Daten.

Wo im Einzelfall die Grenze zwischen „noch personenbezogen“ und „bereits anonymisiert“ verläuft, ist datenschutzrechtlich umstritten und höchst einzelfallabhängig. Der EuGH hat in der Breyer-Entscheidung (EuGH, Urteil vom 19.10.2016, C-582/14) definiert, dass es darauf ankommt, ob Mittel existieren, die von der datenverarbeitenden Stelle

> *„nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die bei ihm befindlichen Daten mit den Zusatzinformationen einer anderen Person so zu verknüpfen, dass ihm eine Identifikation der betroffenen Person gelingt.“*

Demnach handelt es sich für die datenverarbeitende Stelle nicht um personenbezogene Daten, wenn

> *„die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar wäre, zum Beispiel, weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung de facto vernachlässigbar erschiene.“ (EuGH, Urteil vom 19.10.2016, C-582/14, Rn. 44)*

Ob und wann dies der Fall ist, ist stets einzelfallbezogen zu bewerten. Je nach Umständen des Einzelfalles wäre also ein Ergebnis denkbar, bei dem die jeweiligen Daten für die eine datenverarbeitende Stelle (z.B. den Verantwortlichen) zwar (nur) pseudonymisiert sind, der Datenempfänger die betroffenen Personen jedoch nicht „mit verhältnismäßigen Mitteln“ identifizieren kann und daher (zumindest für diesen) eine Anonymisierung vorliegt. Diese rechtliche Situation eröffnet Akteuren im Gesundheitsbereich enorme Chancen, durch technische Mittel eine Anonymisierungswirkung zu erreichen. Gleichwohl bleibt es immer eine Frage des Einzelfalles.

16. Dürfen Datensätze des Medizinprodukts an Dritte weitergegeben werden?

→ Jede Weitergabe personenbezogener Daten an einen Dritten stellt eine Datenverarbeitung dar, die einer Rechtsgrundlage bedarf.

Eine Einwilligung liegt oft nahe. Sie hat jedoch rechtliche und praktische Nachteile. Beispielsweise ist sie jederzeit widerruflich und im Massengeschäft oft nicht zweckmäßig. Alternativ kommen im medizinischen Kontext diverse Szenarien in Betracht, in welchen die Daten eines Patienten zulässigerweise weitergegeben werden dürfen.

Wird ein Medizinprodukt im Rahmen der Behandlung eines Patienten eingesetzt, hat der Anbieter eines Medizinproduktes, der dem Arzt/Krankenhaus etwa Cloud- und/oder Wartungsleistungen zur Verfügung stellt, typischerweise die Rolle des Auftragsverarbeiters im Sinne des Art. 28 DS-GVO inne. Dies gilt grundsätzlich auch dann, sofern das Medizinprodukt mit KI-Komponenten arbeitet.

Wenn der Hersteller des Medizinproduktes die Daten über den Zweck der medizinischen Behandlung hinaus verarbeitet, etwa zum Trainieren der KI, ist der Fall anders gelagert.

In diesem Fall verfolgt der Hersteller des Medizinprodukts eigenständige (auch kommerzielle) Zwecke, welche nicht mit der originären medizinischen Behandlung zusammengeführt werden können. Dann bedarf es – anders als bei der Auftragsverarbeitung, bei der die Weitergabe nach Art. 28 DS-GVO privilegiert ist – einer expliziten Rechtsgrundlage. Umstritten ist die Frage, ob der Hersteller des Medizinprodukts ohne Einwilligung der betroffenen Patienten berechtigt ist, die ihm im Rahmen der Auftragsverarbeitung überlassenen Patientendaten zu anonymisieren, um sie im Nachgang zu eigenen Zwecken zu verwenden. Aufsichtsbehörden sehen dies kritisch, eine höchstrichterliche Rechtsprechung zu dieser Frage existiert jedoch (noch) nicht.

17. Müssen Hersteller und Anwender von Medizinprodukten, die KI beinhalten, eine Datenschutz-Folgenabschätzung durchführen?

→ Im Regelfall: Ja.

Dies setzt jedoch voraus, dass dem Hersteller und/oder dem Anwender im konkreten Einzelfall die Rolle des sogenannten datenschutzrechtlichen Verantwortlichen zukommt. Denn eine Datenschutz-Folgenabschätzung wird vom Verantwortlichen der Datenverarbeitung durchgeführt (nicht etwa: vom Auftragsverarbeiter).

Wann eine Datenschutz-Folgenabschätzung genau durchzuführen ist, wird u.a. in Art. 35 Abs. 3 DS-GVO festgehalten. Hiernach ist ein entsprechendes Vorgehen insbesondere dann erforderlich, wenn – was häufig der Fall sein wird – umfangreich besondere Kategorien personenbezogener Daten, also insbesondere Gesundheitsdaten, verarbeitet werden. Daneben haben die Datenschutzaufsichtsbehörden eine sogenannte **Muss-Liste** veröffentlicht, welche ebenfalls **KI-basierte Verarbeitungsvorgänge aufgreift**. Schlussendlich existieren allgemeine risikobeeinflussende Faktoren, welche eine Datenschutz-Folgenabschätzung erforderlich machen können, ohne dass dies ausdrücklich gesetzlich angeordnet ist. Durch die Kombination der hier entscheidenden Faktoren (also die Verarbeitung von Gesundheitsdaten sowie die Nutzung von KI-Komponenten) wird in vielen Fällen „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ zumindest nicht auszuschließen sein.

Eine abweichende Einschätzung ist im konkreten Einzelfall aber möglich. Werden beispielsweise keine oder nur wenige personenbezogene Daten verarbeitet, kann dies die Durchführung einer Datenschutz-Folgenabschätzung entbehrlich machen. Auch technische Besonderheiten – also die konkrete Art der Datenverarbeitung – kann einen entscheidenden Einfluss auf eine vorgeschaltete Risikoeinschätzung entfalten. Diese Einschätzung sollte dann aber in einer sogenannten Schwellwertanalyse dokumentiert werden, um die tragenden Erwägungen gegenüber der Datenschutzaufsichtsbehörde nachweisen zu können (Stichwort: Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO).

Praktische Anwendung auf die Beispielsfälle: Am Beispiel des Medizinprodukts „NeoplasKI“ müsste der Hersteller etwa eine Datenschutz-Folgenabschätzung für den Trainingsprozess der KI durchführen, während es dem Anwender – der Arztpraxis oder dem Krankenhaus – obliegt, eine Datenschutz-Folgenabschätzung für die Nutzungsphase durchzuführen. Die Verantwortlichkeiten und die daraus resultierenden Pflichten müssen also nach den jeweiligen Lebenszyklen der KI und dem hierbei maßgeblichen Einfluss auf die Datenverarbeitung unterschieden werden.

18. Welche Anforderungen gelten in Bezug auf die Datensicherheit?

→ KI-basierte Medizintechnik eröffnet aufgrund ihrer besonderen technischen Eigenschaften neue Angriffspunkte für Cyberangriffe.

Anforderungen an die **Cybersicherheit** ergeben sich aus der MDR/IVDR, dem AI Act und der DS-GVO. Der neue Cyber Resilience Act ist hingegen nicht auf Medizinprodukte nach MDR und IVDR anwendbar.

Nachfolgend ein Überblick:

Die **MDR**, welche den Hersteller von Medizinprodukten adressiert, definiert an mehreren Stellen Anforderungen an die Cybersicherheit. Gemäß Art. 5 Abs. 2 MDR muss ein Produkt unter Berücksichtigung seiner Zweckbestimmung den in Anhang I festgelegten grundlegenden Sicherheits- und Leistungsanforderungen genügen. Produkte müssen so konzipiert sein, dass sie sicher und wirksam sind. Dabei ist der „allgemein anerkannte Stand der Technik“ zugrunde zu legen. Anhang I Abschnitt 14.2. lit. (d) MDR schreibt vor, dass Produkte so entwickelt werden, dass Risiken im Zusammenhang mit möglichen negativen Wechselwirkungen zwischen Software und der IT-Umgebung, in der sie eingesetzt wird und mit der sie interagiert, so weit wie möglich reduziert werden. Ferner hat der Hersteller nach Anhang I Abschnitt 17.4. MDR Mindestanforderungen bezüglich Eigenschaften von IT-Netzen und IT-Sicherheitsmaßnahmen einschließlich des Schutzes vor unbefugtem Zugriff festzulegen, die für den bestimmungsgemäßen Einsatz der Software erforderlich sind. Die **IVDR** enthält insoweit inhaltlich und wörtlich im Wesentlichen dieselben Anforderungen wie die MDR (vgl. z.B. Art. 5 Abs. 2, Anhang I Abschnitte 1 und 16.2).

Die obigen Vorschriften bleiben recht abstrakt, erfahren aber eine Konkretisierung durch die **Leitlinie der Medical Device Coordination Group (MDCG) 2019-16 „Guidance on Cybersecurity for medical devices“** (Link). Deren Zweck besteht darin, Herstellern eine Orientierungshilfe zur Umsetzung der cyberbezogenen Anforderungen der MDR und IVDR zu geben. Die Leitlinie ist zwar rechtlich unverbindlich, aber insofern relevant, als sie vom EuGH in Rechtsstreitigkeiten zur Auslegung herangezogen werden kann. Außerdem prüfen die Benannten Stellen die MDR- bzw. IVDR-Konformität in der Regel anhand der MDCG Guidance-Dokumente, sodass Struktur und Inhalt der Technischen Dokumentation den MDCG-Vorgaben entsprechen sollte. Hersteller sollten ihr somit entsprechende Beachtung schenken.

Ergänzend können Hersteller und Anwender ein kürzlich **vom BSI veröffentlichtes Papier unter dem Titel „AI Security concerns in a nutshell“** heranziehen. Darin werden die wichtigsten Arten von Cyberangriffen, die speziell auf KI-Systeme abzielen, dargestellt und jeweils mögliche Verteidigungsmaßnahmen vorgestellt (Link).

Der **AI Act** ergänzt die Anforderungen der MDR und IVDR. Anbieter von Hochrisiko-KI-Systemen, wozu in vielen Fällen KI-basierte Medizinprodukte zählen, müssen insbesondere die in Art. 15 AI Act definierten Anforderungen an die Robustheit und Cybersicherheit von KI-Systemen erfüllen. Hierzu zählt, dass die technischen Lösungen zur Gewährleistung der Cybersicherheit von Hochrisiko-KI-Systemen, zu denen praktisch alle KI-Systeme in der Medizintechnik zählen (siehe Frage 5), „den jeweiligen Umständen und Risiken angemessen sind“. Betreibern von solchen Hochrisiko-KI-Systemen (z.B. Krankenhäuser, Arztpraxen) legt Art. 26 AI Act die Verpflichtung zum Einsatz von angemessenen technischen und organisatorischen Maßnahmen auf, um sicherzustellen, dass die KI-Systeme entsprechend der Gebrauchsanweisung genutzt werden.

Die **DS-GVO** definiert Anforderungen an die IT-Sicherheit vor allem in Art. 32 DS-GVO. Demnach müssen der Verantwortliche (oftmals das Krankenhaus bzw. die Arztpraxis) und der Auftragsverarbeiter (dies kann – je nach Fallkonstellation – der Hersteller des Produktes sein, der z.B. per Fernzugriff Zugang zu personenbezogenen Daten erhält) „geeignete technische und organisatorische Maßnahmen" treffen, um ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten. Dabei sind u.a. der Stand der Technik, die Implementierungskosten und Art, Umfang, Umstände und der Zwecke der Verarbeitung zu berücksichtigen. Flankierend zu Art. 32 DS-GVO sind für Betreiber Kritischer Infrastrukturen (hierunter können Krankenhäuser fallen) § 8a BSI-Gesetz und der Branchenspezifische Sicherheitsstandard (B3S) zu beachten (Link).

Wie stets im IT-Sicherheitsrecht müssen Vorschriften – die regelmäßig recht abstrakt gehalten werden – in der Praxis mit Leben gefüllt werden. Dies erfordert ein interdisziplinäres Zusammenwirken aus Juristen und IT-Sachverständigen.

Praktische Anwendung auf die Beispielsfälle: Wie bereits angeführt, adressieren die MDR/IVDR zunächst den Hersteller eines Medizinprodukts. Auch der AI Act sieht gerade für Anbieter von Hochrisiko-KI-Systemen gewisse Verpflichtungen zur IT-Sicherheit vor. Es ist somit zunächst die originäre Aufgabe der Hersteller von „NeoplasKI" bzw. „Blusser", eben diese Verpflichtungen bei der Konzeption ihrer Medizinprodukte umzusetzen.

Eine spannende Rolle nimmt daneben der Anwender von „NeoplasKI" ein (etwa die Arztpraxis oder das Krankenhaus), welcher zumindest in der Nutzungsphase regelmäßig der Verantwortliche ist. Art. 25 DS-GVO („Privacy by Design" und „Privacy by Default") sowie Art. 32 DS-GVO sehen insoweit spezifische Pflichten vor, welche den technischen Datenschutz abbilden. Problematisch ist hierbei jedoch, dass der Anwender keinen originären Einfluss auf die technische Konzeption des Medizinprodukts hat.

Aus den vorgenannten Regelungen resultiert daher letztlich eine „Auswahlentscheidung" des Anwenders dahingehend, welcher Hersteller eines Medizinprodukts die Einhaltung der Anforderungen der DS-GVO überhaupt **ermöglicht**. Während dies für die Auftragsverarbeitung gemäß Art. 28 DS-GVO ohnehin gesetzlich vorgeschrieben wird, gelten die vorgenannten Grundsätze letztlich für den gesamten Verarbeitungszyklus unter Nutzung eines KI-gestützten Medizinprodukts. Aus Sicht eines Herstellers liegt es daher auf der Hand, dass die rechtskonforme Technikgestaltung nicht nur der Umsetzung der eigenen rechtlichen Verpflichtungen dient, sondern mitunter einen direkten Einfluss auf die Wirtschaftlichkeit des Medizinprodukts entfalten kann. Der Hersteller von „NeoplasKI" ist daher gut beraten, bereits bei der Konzeption des Medizinprodukts auch den Blickwinkel des künftigen Anwenders einzunehmen. Durch die Erleichterung der Einhaltung der Datenschutzanforderungen für den Nutzer kann sich der Hersteller insoweit einen echten Marktvorteil verschaffen.

19. Welche Anforderungen gelten in Bezug auf die Transparenz?

→ Der Grundsatz der Transparenz spielt im Datenschutzrecht eine herausragende Rolle. Die verantwortliche Stelle hat diesen Grundsatz auf gleich mehreren Ebenen zu berücksichtigen, weshalb das Verständnis über die Datenverarbeitung letztlich als Grundvoraussetzung zur Einhaltung der DS-GVO angesehen werden kann. Gerade wenn KI-Komponenten zum Einsatz kommen, kann die Umsetzung dieser Anforderungen jedoch mitunter schwierig sein, da die Funktionsweisen und Entscheidungswege von KI häufig nicht ohne Weiteres verständlich sind (sogenannter „Black Box"-Gedanke).

In einem ersten Schritt muss der Verantwortliche die **Datenverarbeitung zunächst nachvollziehen**, um die formellen Anforderungen der DS-GVO überhaupt umsetzen zu können. Dies betrifft etwa den Eintrag im Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO sowie das Durchführen einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO. Ohne das nötige Verständnis zur Funktionsweise des Medizinprodukts, wird es dem Verantwortlichen nicht möglich sein, diese Pflichten umzusetzen. Daneben ist die verantwortliche Stelle gegenüber der Datenschutzaufsichtsbehörde nachweispflichtig (vgl. Art. 5 Abs. 2 DS-GVO). Die vorgenannten Pflichten gelten dabei sowohl für den Hersteller als auch für den Anwender des Medizinprodukts – jeweils soweit eine datenschutzrechtliche Verantwortlichkeit anzunehmen ist.

Auch spielt der Grundsatz der **Transparenz im Verhältnis zu betroffenen Personen** eine herausragende Rolle. Während in Art. 13 Abs. 1 DS-GVO bereits eine Vielzahl an Informationen festgelegt werden, welche den betroffenen Personen bereitzustellen sind, muss auch eine etwaige Einwilligungserklärung (beispielsweise von Patienten) „in informierter Weise" erfolgen. In beiden Fällen stellt sich jedoch die Frage, wie weitreichend diese Informationen ausgestaltet sein müssen. Obgleich die Einzelheiten hierzu höchst umstritten sind, wird es im Ergebnis auf einen verständlichen und gleichsam pragmatischen Lösungsansatz hinauslaufen (müssen). Nach unserer Einschätzung muss über den hinter dem KI-System stehenden Algorithmus selbst nicht informiert werden, da dieser als Geschäftsgeheimnis zu klassifizieren ist. Dennoch muss betroffenen Personen klar vor Augen geführt werden, welche Verarbeitungsschritte unter Nutzung einer KI vorgenommen werden und auf welcher Basis der Output (also das Ergebnis) der KI bestimmt wird. Während der Hersteller etwa alle vom Trainieren des KI-Systems betroffenen Personen zu informieren hat, wird der Anwender insbesondere gegenüber Patienten zur Information verpflichtet.

In letzterem Fall ist jedoch insbesondere klärungsbedürftig, wie der Anwender des Medizinprodukts diese Informationen überhaupt in Erfahrung bringen kann. Dies betrifft insbesondere Angaben zur technischen Funktionsweise des KI-gestützten Medizinprodukts, welche häufig nicht ohne Weiteres zur Verfügung stehen. Einen gewissen „Rettungsanker" liefert insoweit der **AI Act**, als er **dem Anbieter eines Hochrisiko-KI-Systems in dessen Artikel 13 hohe Transparenzpflichten auferlegt**. So muss insbesondere sichergestellt sein, dass der Anwender die Ergebnisse des Hochrisiko-KI-Systems interpretieren kann und diesem eine Gebrauchsanweisung zur Verfügung gestellt wird. Diese Gebrauchsanweisung muss bestimmte Mindestangaben beinhalten, wobei insgesamt ein „angemessenes Maß" an Transparenz zu gewährleisten ist.

Die Einhaltung von Art. 13 AI Act spielt darüber hinaus auch in der Konformitätsbewertung eines KI einsetzenden Medizinprodukts bzw. IVD eine große Rolle und ist Zertifizierungsvoraussetzung sowohl für das KI-System als auch für das Medizinprodukt bzw. IVD (siehe Frage 6).

Neben diesen ohnehin verpflichtend vorgesehenen Informationen sollten Hersteller entsprechender Medizinprodukte von vornherein so transparente Informationen wie möglich zur Verfügung stellen. Dies verfolgt insbesondere den Zweck, dass der Anwender, wie bereits ausgeführt, die Pflichten der DS-GVO überhaupt umsetzen **kann**. Soweit Hersteller von Medizinprodukten die Fragestellungen des Anwenders bereits bei der Konzeption und Vermarktung mitdenken, kann dies somit zu einem echten Verkaufsargument werden.

20. Was heißt das alles für die praktische Herangehensweise von Medizinprodukteanbietern, die KI-Systeme einsetzen wollen?

→ Die Ausführungen in diesem Whitepaper zeigen: **KI-Systeme in Medizinprodukten erfordern einen multidisziplinären Blickwinkel, Expertise in zahlreichen Spezialgebieten und vor allem Schnittstellenkompetenzen**. Mit regulatorischem Wissen zur MDR und IVDR allein kommt man beim Einsatz von KI in Medizinprodukten und IVD nicht mehr weiter. Die Erfüllung der Anforderungen des AI Act, die Konformitätsbewertung von KI-Systemen und der starke IT- und Datenschutzbezug können in der Praxis nur durch ein Team von Experten mit vertieftem Fachwissen in ihrem jeweiligen Gebiet, der Fähigkeit und Bereitschaft zur intensiven Zusammenarbeit und der nötigen Sensibilität für die Zusammenführung der Informationen und Ergebnisse an den Schnittstellen bewältigt werden. Hier ist enges Teamwork von Regulatorik-, Medizintechnik-, KI-, IT-, Cybersecurity- und Datenschutzexperten gefragt – sowohl auf der rechtlichen als auch auf der fachlichen Ebene.

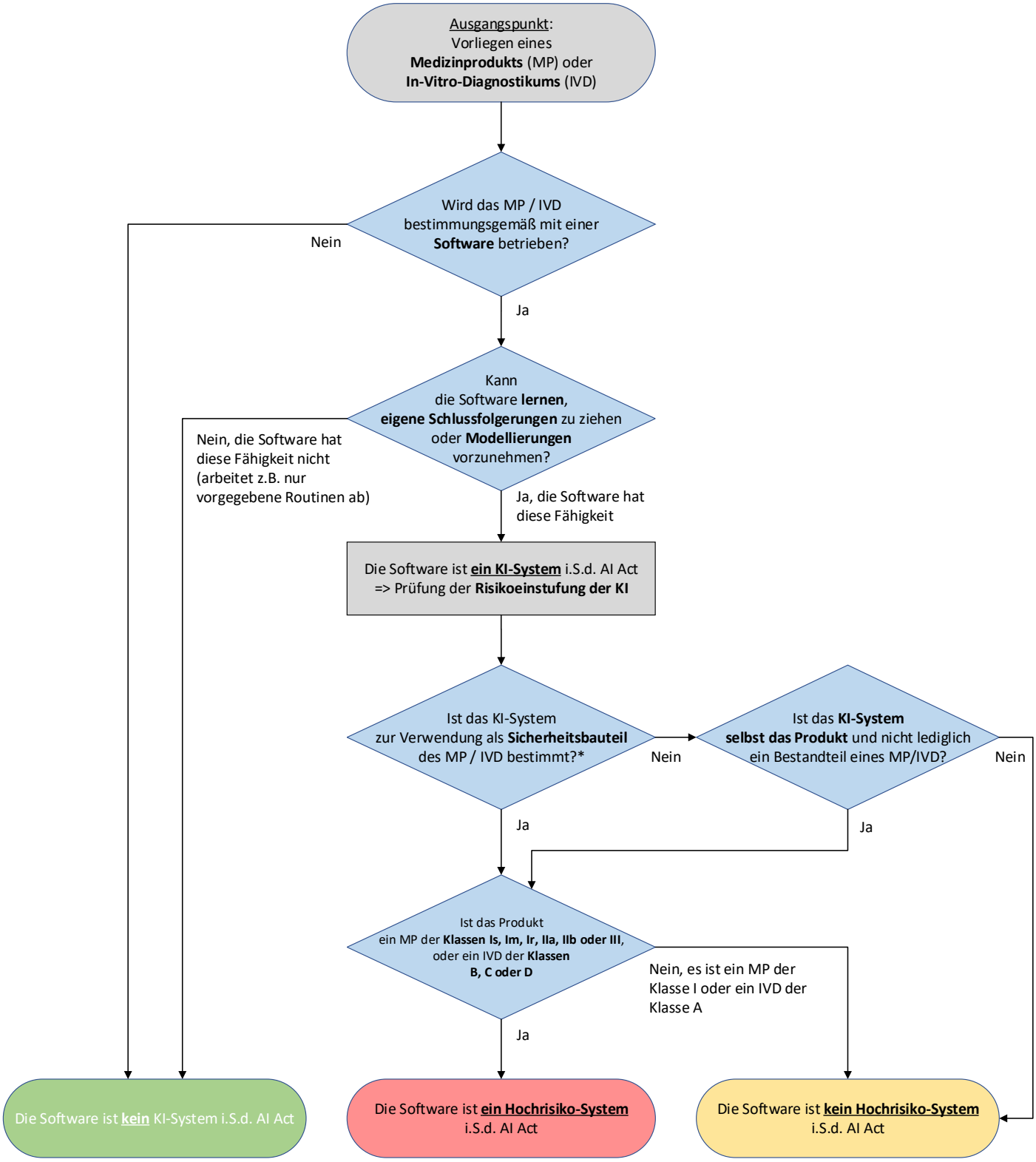
Auch für die neue KI-Regulatorik wird IT-Wissen allein nicht genügen. Das Konformitätsbewertungsverfahren und Zertifizierungssystem nach dem AI Act sind stark an die Medizinprodukteregulatorik angelehnt und für den „klassischen" IT- und Datenschutzbereich ein völlig neues System. Inhouse-Teams und Berater, die Know-How in der Medizinprodukteregulatorik und in den IT- und Datenschutzthemen vereinen und deshalb ganzheitliche Lösungen aus einer Hand liefern können, sind hier klar im Vorteil.

Für die Unternehmensorganisation bedeutet das in der Praxis:

Regulatory Affairs im KI-Zeitalter erschöpft sich nicht mehr in der detaillierten Kenntnis der MDR bzw. IVDR und ihrer praktischen Anwendung – künftig werden in diesem Bereich noch weitere Experten vor allem aus dem IT-, Cybersecurity- und Datenschutzbereich gebraucht, um vollumfänglich compliant zu sein. Hersteller von Medizinprodukten und IVD mit KI-Systemen sollten deshalb bei der Zusammenstellung ihrer Inhouse-Teams und Berater auf einen multidisziplinären Ansatz und die Abdeckung der benötigten Schnittstellenkompetenz achten und jede Produktentwicklung von Anfang an ganzheitlich in diesem Sinn angehen. Dies vermeidet Probleme und Brüche z.B. innerhalb des einheitlichen Konformitätsbewertungsverfahrens für Medizinprodukte und KI-Systeme ebenso wie datenschutzrechtliche Fehler in der Trainingsphase der KI oder bei der Anwendung in der Praxis. Wer sich hier personell – intern und extern – richtig aufstellt, für den bieten Medizinprodukte und IVD mit KI-Systemen eine einmalige Chance für die Zukunft.

Prüfschema

Vorliegen eines KI-Systems gemäß AI Act und Risikoeinstufung des KI-Systems bei Medizinprodukten und In-Vitro-Diagnostika



*Ein Sicherheitsbauteil liegt im Zweifel vor, wenn das KI-System eine Sicherheitsfunktion erfüllt oder dessen Ausfall oder Fehlfunktion die Gesundheit oder Sicherheit von Personen oder Gegenständen gefährdet.

Checkliste

zu den formellen Anforderungen der DS-GVO

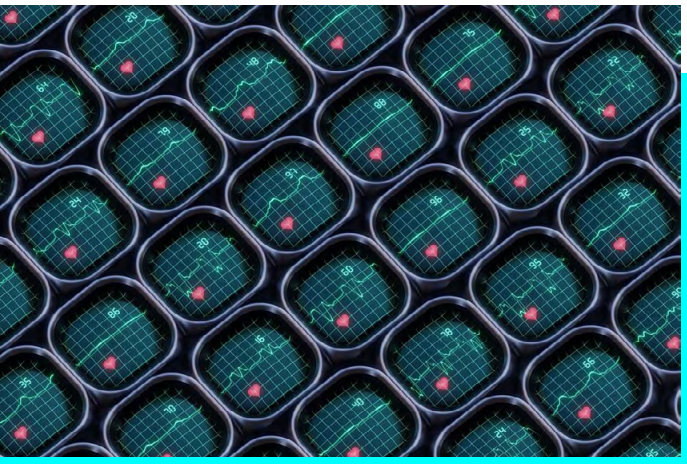
Um die formellen Anforderungen der DS-GVO möglichst rechtssicher umsetzen zu können, sollten Hersteller und Anwender von intelligenten Medizinprodukten insbesondere die nachstehend aufgezeigten Dokumentations- und Prüfschritte durchführen. Zur besseren Lesbarkeit wird nachstehend einheitlich von der Nutzung des Medizinprodukts gesprochen. Die grundlegenden datenschutzrechtlichen Anforderungen sind jedoch in jedem Lebenszyklus eines KI-gestützten Medizinprodukts zu beachten, also sowohl in der Trainingsphase, als auch in der sich hieran anschließenden Nutzungsphase. Die Anforderungen der DS-GVO adressieren daher den Hersteller und Nutzer des Medizinprodukts gleichermaßen, zumindest soweit eine datenschutzrechtliche Verantwortlichkeit besteht.

Folgende Fragen sind bei der Nutzung eines KI-gestützten Medizinprodukts zu klären:

- ☐ Sind die wesentlichen Verarbeitungsvorgänge und Datenströme unter Nutzung des Medizinprodukts bekannt und wurden diese dokumentiert?
- ☐ Besteht ein hinreichendes (technisches) Verständnis zur grundlegenden Funktionsweise der eingesetzten KI-Komponenten?
- ☐ Wurde geprüft, ob und inwieweit personenbezogene Daten unter Nutzung des Medizinprodukts verarbeitet werden?
- ☐ Wurde geprüft und dokumentiert, ob und inwieweit auch anonymisierte, pseudonymisierte oder synthetische Daten für den jeweiligen Einsatzzweck des Medizinprodukts verwendet werden könnten?
- ☐ Wurde geprüft, ob die allgemeinen Grundsätze des Art. 5 Abs. 1 DS-GVO (technisch) umgesetzt werden können und dies gemäß Art. 5 Abs. 2 DS-GVO gegenüber der Datenschutzaufsichtsbehörde nachgewiesen werden kann?
- ☐ Wurde das Vorliegen einer datenschutzrechtlichen Rechtsgrundlage geprüft und dokumentiert? Wurde hierbei eine etwaige Zweckänderung gemäß Art. 6 Abs. 4 DS-GVO berücksichtigt?
- ☐ Werden betroffenen Personen aussagekräftige Datenschutzhinweise gemäß Art. 13, 14 DS-GVO ausgeteilt?
- ☐ Existiert ein schriftliches Rechte- und Rollenkonzept, welches den Zugang zu den jeweiligen personenbezogenen Daten vorgibt?
- ☐ Sind Mechanismen vorgesehen, welche die Ausübung von Betroffenenrechten gemäß den Art. 15 ff. DS-GVO (Auskunft, Berichtigung, Löschung, etc.) ermöglichen?
- ☐ Wurde geprüft, ob und inwieweit eine automatisierte Entscheidungsfindung gemäß Art. 22 Abs. 1 DS-GVO vorgenommen wird, und ob dies datenschutzrechtlich zulässig ist?
- ☐ Wurde die Datenverarbeitung unter Nutzung des Medizinprodukts in das Verarbeitungsverzeichnis gemäß Art. 30 DS-GVO übertragen?
- ☐ Wurden angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO zur Wahrung der Rechte und Freiheiten der betroffenen Personen ergriffen?
- ☐ Existiert ein Maßnahmenplan, wie im Falle einer Verletzung des Schutzes personenbezogener Daten gemäß den Art. 33, 34 DS-GVO umzugehen ist?
- ☐ Wurde eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO durchgeführt?
- ☐ Wurden etwaige Vertragsverhältnisse mit weiteren Beteiligten (Dienstleister, konzernverbundene Unternehmen, etc.) abgeschlossen und auf deren Datenschutzkonformität geprüft?
- ☐ Wurde geprüft, ob und inwieweit ein Drittlandtransfer im Sinne der Art. 44 ff. DS-GVO stattfindet? Wurde ggf. ein Transfer Impact Assessment durchgeführt?
- ☐ Wurde der Datenschutzbeauftragte frühzeitig in die datenschutzrechtliche Prüfung einbezogen?

Unsere Fokusgruppe Digital Health:

Meistern Sie die Herausforderungen der Digitalisierung im Gesundheitssektor mit SKW Schwarz



Die Digitalisierung der Gesellschaft schreitet weiter voran und macht auch vor der Gesundheitsbranche keinen Halt. Mehr noch: Im Bereich Life Sciences & Health ist die Digitalisierung eine der zentralen Herausforderungen und Chancen für Unternehmen in den nächsten Jahren. Dieser Veränderungsprozess benötigt Expertise in der stetig komplexer werdenden Regulatorik, ein tiefes Verständnis der zugrundeliegenden Rechtsgebiete und deren Schnittstellen, verbunden mit der notwendigen Innovationskraft und Kreativität, die wir als Kanzlei vereinen.

Transformieren Sie die Gesundheitsbranche mit uns:

Unsere Spezialistinnen und Spezialisten beraten Sie bei Ihren Herausforderungen – Digitalisierung ist unsere Kernexpertise.

Wir denken weiter und vereinen mit unserer Ausrichtung auf die Bereiche Life Sciences & Health, ITD und IP in unserer Fokusgruppe „Digital Health“ alle relevanten Gebiete für die Digitalisierung des Gesundheitssektors von Know-how in Regulatorik und Compliance, IT-, IP- und Datenschutzrecht bis zu Vergabe- Handels- und Gesellschaftsrecht. Damit ist SKW Schwarz ihr idealer Ansprechpartner in allen Bereichen rund um das Thema „Digital Health“. Wir führen das Wissen und die Erfahrung unserer Expertinnen und Experten für Ihre Digitalisierungsvorhaben zu einer Beratung aus einer Hand zusammen.

Innovative digitale Produkte und Dienstleistungen im Gesundheitssektor können unsere Gesellschaft nachhaltig verändern. Wir unterstützen Sie von der Gründung bis zur Transaktion, mit einem ganzheitlichen Blick und Expertenwissen in den Bereichen Life Sciences & Health, Gesellschaftsrecht sowie IT- und Datenschutzrecht.

Ob Digitalisierung von Medizinprodukten, rechtssichere Lösungen für KI-Einsatz, Ausschreibungen digitaler Gesundheitsleistungen oder die Entwicklung von Health-Apps und DiGAs – unser Team steht Ihnen mit umfassendem Know-how zur Seite. Wir helfen Ihnen außerdem, die komplexen rechtlichen Anforderungen im Social Media Marketing und der Digitalisierung im Krankenhauswesen zu meistern.

Erfahren Sie mehr über unsere Fokusgruppenarbeit und sichern Sie sich unsere exklusiven Whitepapers zur Healthcare Compliance und Datenschutz bei Medizinprodukten auf unserer Landingpage. Kontaktieren Sie uns für weiterführende Informationen und lassen Sie sich von unserer Expertise überzeugen.

Unsere Expertinnen und Experten
für Digital Health

Dr. Oliver Stöckel
Partner

+49 89 28640-255
o.stoeckel@skwschwarz.de

Afra Nickl
Associate

+49 89 28640-255
a.nickl@skwschwarz.de

Fabian Bauer, LL.M.
Counsel

+49 69 630001-82
f.bauer@skwschwarz.de

Marius Drabiniok
Associate

+49 69 630001-65
m.drabiniok@skwschwarz.de

10719 Berlin
Kranzler Eck
Kurfürstendamm 21
T +49 30 8892650-0
F +49 30 8892650-10

60598 Frankfurt/Main
Mörfelder Landstraße 117
T +49 69 630001-0
F +49 69 6355-22

20459 Hamburg
Ludwig-Erhard-Straße 1
T +49 40 33401-0
F +49 40 33401-530

80333 München
Wittelsbacherplatz 1
T +49 89 28640-0
F +49 89 28094-32

skwschwarz.de