Anmerkungen zum Vorschlag für die EU-Verordnung zur künstlichen Intelligenz vom 21. April 2021

Prof. Dr. Martin Haimerl
Wissenschaftlicher Direktor
Innovations- und Forschungs-Centrum Tuttlingen der Hochschule Furtwangen (IFC)
E-Mail: Martin.Haimerl@hs-furtwangen.de

Hochschule Furtwangen | Furtwangen University
Hochschulcampus Tuttlingen
Kronenstraße 16
78532 Tuttlingen

Inhalt der KI-Verordnung	Feedback
Anhang I Zu den Verfahren der künstlichen Intelligenz zählen nicht nur das maschinelle Lernen, sondern auch: *– Logik- und wissensgestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme;* *– Statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden.*	Dieser bereite Anwendungsbereich kann dazu führen, dass viele Medizinprodukte (und auch andere Produkte), die Software enthalten, in den Anwendungsbereich der KI-Richtlinie fallen, obwohl sie nicht wirklich eine KI- und insbesondere keine Machine Learning-Komponente enthalten. Jeder in Software gegossene Entscheidungsbaum wäre demnach ein KI-System. Da die Verordnung in vielen der Aspekte auf Machine Learning-Verfahren bzw. allgemein auf statistische Ansätze ausgerichtet ist, ist es nicht ersichtlich, warum die gestellten Anforderungen für alle der gelisteten Verfahren gelten sollen. In vielen Fällen wären sie einfach nicht umsetzbar. Eine pauschale Übertragung der Anforderungen in der bisherigen Form auf alle diese Varianten erscheint daher nicht als sinnvoll. Hierzu müsste die Verordnung selbst, insbesondere im Bereich der Umsetzungsanforderungen, an die jeweiligen Verfahren angepasst werden. Manche Aspekte, wie die Einschränkungen/Verbote bestimmter Anwendungsbereiche, sind in der pauschalen Form anwendbar.
Die KI-Verordnung greift einige Begriffe auf, ohne dass sie diese entweder gar nicht, nicht passend oder nicht konsistent mit anderen Verordnungen (wie z.B. der EU-Medizinprodukteverordnung (MDR) einführt. Dazu gehören Begriffe wie z.B. • *„Sicherheitskomponente“ („safety component“)*	Beispiel *„Sicherheitskomponente“ („safety component“)* Die Verordnung definiert diesen Begriff, indem sie den nicht definierten Begriff einer Sicherheitsfunktion verwendet: Eine „Sicherheitskomponente eines Produkts oder Systems“ ist ein *Bestandteil eines Produkts oder Systems, der eine Sicherheitsfunktion für*

• *„fehlerfrei“ und „vollständig“ in Bezug auf Daten („free of error“ und „complete“)* • *„Menschliche Aufsicht“ („Human Oversight“)* • *„Validierung („Validierung“)* • *„SW Update“*	*dieses Produkt oder System erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Sachen gefährdet;* Es bleibt unklar, was eine Sicherheitsfunktion ist. Beispielsweise könnte es eine Funktion sein, die die Sicherheit von Patienten gefährdet, wenn sie sich nicht spezifikationsgemäß verhält. Es könnte aber auch eine Funktion gemeint sein, die eine risikominierende Maßnahme implementiert. Damit bleibt auch der zentrale Begriff der Sicherheitskomponente undefiniert. Ähnliche Unklarheiten verbleiben bei den anderen genannten Begriffen. Da diese in den anderen Punkten dieser Aufstellung aufgegriffen werden, wird auf diese Punkte verwiesen.
Die KI-Richtlinie schließt explizit Medizinprodukte (gemäß Medizinprodukteverordnung / Medical Device Regulation – MDR) und IVD-Produkte (In-Vitro-Diagnostics Regulation – IVDR) mit ein.	Dadurch gibt es eine Doppelung an Anforderungen zwischen der KI-Verordnung und der MDR / IVDR. MDR und IVDR fordern beispielsweise bereits Cybersecurity, ein Risikomanagement, die Post-Market Surveillance, ein Meldesystem, eine technische Dokumentation, ein QM-System usw. Es ist dabei von zentraler Bedeutung, dass keine Inkonsistenzen zwischen den jeweiligen Verordnungen enthalten sind, die dann dazu führen würden, dass manche Vorgehensweisen nicht mehr oder nur unter erheblichem Mehraufwand möglich wären. In der aktuellen Form sind aber noch eine ganze Reihe an derartigen Inkonsistenzen vorhanden, wie einige der im Weiteren gelisteten Punkte aufzeigen.
Die KI-Verordnung gilt unabhängig davon, für was die KI im Medizinprodukt eingesetzt wird.	In Erwägungsgrund (14) wird folgende Anforderung aufgeführt: *„Um ein verhältnismäßiges und wirksames verbindliches Regelwerk für KI-Systeme einzuführen, sollte ein klar definierter risikobasierter Ansatz verfolgt werden. Bei diesem Ansatz sollten Art und Inhalt solcher Vorschriften auf die Intensität und den Umfang der Risiken zugeschnitten werden, die von KI-Systemen ausgehen können.“* Weiterführend wird in Erwägungsgrund (14) *angegeben: „Als hochriskant sollten nur solche KI-Systeme eingestuft werden, die erhebliche schädliche*

	Auswirkungen auf die Gesundheit, die Sicherheit und die Grundrechte von Personen in der Union haben;“ Allerdings wird in dem Vorschlag für die KI-Verordnung selbst ein pauschaler branchenweiter Ansatz verfolgt, bei dem die Anforderungen für Medizinprodukte und andere als Hochrisikoprodukte klassifizierte KI-Systeme unabhängig von ihrem tatsächlichen Risiko pauschal definiert werden. Das gilt z.B. auch für KI-Komponenten, die nicht oder nur sehr bedingt mit Risiken in Verbindung stehen wie z.B. eine KI, die Optimierungen des Energieverbrauchs bei einem Medizinprodukt umsetzt. Unter einem risikobasierten Ansatz ist im Kern zu verstehen, dass das Maß der umzusetzenden Qualitätsmanagementanforderungen in Abhängigkeit von der Risikobewertung umzusetzen ist. Das heißt, dort wo das Risiko bei einem gegebenen Produkt / in Bezug auf eine gegebene Komponente groß ist, dort sind hohe Anforderungen zu erfüllen. Dort wo kein oder nur ein geringes Risiko vorhanden sind, dürfen sie unter Berücksichtigung der Sicherheit des Gesamtprodukts entsprechend angepasst werden. Ein solcher Ansatz ist jedoch in dem vorliegenden Entwurf nicht gegeben. Es wird im Kern lediglich eine pauschale Unterscheidung nach Branchen vorgenommen und nicht gemäß der Sicherheit der jeweils gegebenen Produkte.
Die Anforderungen in der KI-Verordnung gelten nur für Hochrisiko-Produkte.	Es wäre zu überlegen, ob jedes KI-basierte Produkt grundlegende Schritte wie eine Zweckbestimmung definieren muss und darauf aufbauend eine Bewertung dokumentieren muss, ob es sich um ein Hochrisikoprodukt handelt oder nicht. Zu dieser Prüfung sollte im Grunde jedes KI-Produkt verpflichtet sein und das sollte auch entsprechend dokumentiert sein. Alle weiteren Anforderungen könnten entfallen, sofern das Produkt als Nicht-Hoch-Risiko-Produkt einzuordnen ist. Der Prozess könnte durch die Vorlage eines entsprechenden Formblatts unterstützt werden. Eine solche abgestufte Vorgehensweise würde auch in dieser Hinsicht einem risiko-basierten Ansatz besser entsprechen, wie er in dem

	vorherigen Punkt diskutiert wurde. Insgesamt geht es darum, auf Basis einer soliden Begründung den Umfang der umzusetzenden Anforderungen dem Risiko entsprechend anpassen zu können. In den grundlegenden Entscheidungsoptionen zur Vorbereitung der Verordnung scheint eine solche Option nicht wirklich vorhanden gewesen zu sein.
In der Einleitung wird von Maßnahmen gesprochen, mit denen bei KI-Systemen *„sowohl der Nutzen als auch die Risiken der KI auf Unionsebene angemessen geregelt werden“*. Auch in dem White Paper der „HLEG AI“ wird einem ausgewogenen Verhältnis von Risiken und Nutzen eine wichtige Rolle zugeordnet. Die KI-Verordnung selbst betrachtet nur die Seite der Risiken und erlaubt keine Abwägung gegenüber dem potenziellen Nutzen, der sich aus einem System ergibt.	In der EU-Medizinprodukteverordnung (MDR) ist gezielt der folgende Punkt mit aufgenommen: *„… wobei etwaige Risiken im Zusammenhang mit ihrer Anwendung gemessen am Nutzen für den Patienten vertretbar und mit einem hohen Maß an Gesundheitsschutz und Sicherheit vereinbar sein müssen.“* (Anhang I – *Grundlegende Sicherheits- und Leistungsanforderungen*, Kap. 1, Pos. 1). Das würde zu Inkonsistenzen führen, da die KI-Verordnung eine solche Abwägung nicht erlaubt. Gerade in Zeiten der CoViD-Pandemie ist deutlich geworden, dass manchmal Risiken akzeptiert werden müssen, um einen bestimmten Nutzen erreichen zu können, siehe z.B. beschleunigte Zulassung von Impfstoffen. Auch wenn es sich in dem Beispiel um ein Pharma- und nicht um ein Medizinprodukt handelt, zeigt es, wie wichtig eine solche Gegenüberstellung von Risiken und Nutzen ist. Andere Beispiele, die in den Bereich KI hineinreichen, wären Systeme zur Vorhersage und zum Management der Ausbreitung der Infektionen. Es wäre sinnvoll, zu erlauben, eine solche Risiko-Nutzen-Abschätzung machen zu können, wenn entsprechende Begründungen/Nachweise für den Nutzen dargelegt werden können – alleine schon um Konsistenz mit der MDR zu erreichen. Der Ansatz, hier über Ausnahmegenehmigungen gehen zu müssen und dabei die Notwendigkeit eines Konformitätsbewertungsverfahren aussetzen zu können (siehe Erwägungsgrund (68*): „Es ist daher angebracht, dass die Mitgliedstaaten aus außergewöhnlichen Gründen der öffentlichen Sicherheit, des Schutzes des Lebens und der Gesundheit natürlicher Personen und des Schutzes des gewerblichen und kommerziellen Eigentums das Inverkehrbringen oder die Inbetriebnahme von KI-Systemen, die keiner Konformitätsbewertung*

	unterzogen wurden, genehmigen könnten."), erscheint hier nicht ausreichend.
In Art. 9 (4a) wird eine *„weitestmögliche Beseitigung oder Verringerung der Risiken durch eine geeignete Konzeption und Entwicklung"* gefordert, d.h. eine Reduzierung der Risiken *„as far as possible"*.	Eine solche Formulierung führt dazu, dass viele KI-Systeme nie fertig entwickelt werden können, da eine weitere Reduzierung von Risiken bei einem mit Risiken verbundenen Produkt i.d.R. möglich ist und dazu führen würde, dass Risiken ohne ein wirkliches Ende immer weiter reduziert werden müssen. Stattdessen sollte es genügen, ein der Zweckbestimmung angemessenes Niveau der Risiken zu erreichen. Aus diesem Grund ist in der EU-Medizinprodukteverordnung (MDR) die Anforderung in angepasster Form vorhanden. Dort ist angegeben: *„Die in diesem Anhang dargelegte Anforderung zur möglichst weitgehenden Minimierung von Risiken ist so zu verstehen, dass Risiken so weit zu verringern sind, wie es ohne negative Auswirkungen auf das Nutzen-Risiko-Verhältnis möglich ist."* (Anhang I – *Grundlegende Sicherheits- und Leistungsanforderungen*, Kap. 1, Pos. 2). Die Anforderung *„weitestmöglich"* bzw. *„as far as possible"* sollte aus Gründen der Machbarkeit und aus Konsistenzgründen zur MDR in der KI-Verordnung entsprechend angepasst werden.
Die Verordnung spricht regelmäßig von *„Validierung"* (*„validation"*), meint dabei in der Regel aber nur die Modellvalidierung von KI-Systemen. Diese Begrifflichkeiten treten mehrfach auf in Zusammenhang mit *„Trainings-, Validierungs- und Testdaten"*. An manchen Stellen wird auch von *Trainings-, Test- und Validierungsverfahren* (Erwägungsgrund 46), von *Untersuchungs-, Test- und Validierungsverfahren* (Art. 17), *Entwicklung, Erprobung und Validierung* (Art. 53). In Art. 9(6) wird zudem angegeben *„Hochrisiko-KI-Systeme müssen getestet werden, um die am besten geeigneten Risikomanagementmaßnahmen zu ermitteln. Durch das Testen wird sichergestellt, dass Hochrisiko-KI-Systeme stets bestimmungsgemäß*	Der Begriff „Validierung" bezeichnet im Bereich der Entwicklung von Medizinprodukten (und auch in vielen anderen Entwicklungsbereichen) einen möglichst objektiven Nachweis, dass das entwickelte Produkt Anwendungszweck in passender Weise umsetzt. Im Bereich der KI wird der Begriff „*Validierung*" jedoch in der Regel in einem sehr viel eingeschränkteren Sinn verwendet. Er bedeutet hier die Optimierung bzw. Adjustierung (Tuning) von nichttrainierbaren Modellparametern (im Sinne eines „model tunings"). Die in der KI-Verordnung verwendeten Formulierungen und der stetige Bezug auf die Datensätze (*„Validierungsdaten*") zeigen auf, dass die Verordnung den Begriff in diesem eingeschränkten Verständnis verwendet.

funktionieren und die Anforderungen dieses Kapitels erfüllen.“. In Art. 9(5) ist aufgeführt *„Die Testverfahren müssen geeignet sein, die Zweckbestimmung des KI-Systems zu erfüllen, und brauchen nicht über das hierfür erforderliche Maß hinauszugehen.“* und in Art. 9(6) *„Das Testen erfolgt anhand vorab festgelegter Parameter und probabilistischer Schwellenwerte, die für die Zweckbestimmung des Hochrisiko-KI-Systems geeignet sind.“* In Art. 17 (1b) sind *„Techniken, Verfahren und systematische Maßnahmen für den Entwurf, die Entwurfskontrolle und die Entwurfsprüfung des Hochrisiko-KI-Systems;“ („techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system;“) gefordert.*	Bei der Entwicklung von Medizinprodukten (und auch in anderen Bereichen) ist jedoch die Validierung eine Kernaufgabe, ohne die ein Produkt nicht auf den Markt gebracht werden darf. Diese Aufgabenstellung ist in der KI-Verordnung nahezu gar nicht vorhanden. Zumindest ist diese Thematik nicht entsprechend klar dargelegt. Lediglich der Begriff „*Validierungsdaten*“ ist definiert, jedoch nicht Begriffe wie „Validierung“ oder „*Validierungsverfahren*“. Die unterschiedlichen Reihenfolgen und Kombinationen des Begriffs „*Validierungsverfahren*“ in verschiedenen Abschnitten der KI-Verordnung lassen ein wenig vermuten, dass z.T. die klassische Validierung hier ein Stück mitgedacht sein könnte. Das sollte dann aber auch in voller Konsequenz definiert und dargestellt werden. Insgesamt fehlen in der KI-Verordnung Kernelemente der Validierung. Es wird zwar z.B. gefordert, dass Genauigkeitsbereiche Metriken zur Bewertung von KI-Verfahren verwendet und Ergebnisse darüber dokumentiert werden. Es wird in der KI-Verordnung selbst aber nicht darüber gesprochen, dass (im Sinne einer Validierung) schlüssig zu begründen ist, dass diese Metriken geeignet sind, den jeweiligen Anwendungsfall zu bewerten. Auch viele andere Punkte wie Leistungsgrenzen oder Genauigkeitsgraden müssen zunächst nur angegeben, aber nicht begründet werden. Lediglich in Anhang IV (*„Technische Dokumentation“*) – Pos. 2b ist gefordert, dass „*Entwurfsentscheidungen*“ zusammen mit „*Gründen und Annahmen*“ dafür dokumentiert werden müssen und in Art. 13(3), dass eine Kommunikation *„des Maßes an Genauigkeit, Robustheit und Cybersicherheit gemäß Artikel 15, für das das Hochrisiko-KI-System getestet und validiert wurde und das zu erwarten ist“* an den Benutzer erfolgen muss. Ein Nachweis, ob das für die Zweckbestimmung angemessen / ausreichend ist, fehlt auch hier. Die Anforderungen / Hinweise in Art. 9(5), 9(6) und 9(7) zeigen nochmals auf, dass Begriffe hier nicht passend eingeordnet sind. Testverfahren alleine genügen nicht, um die Erfüllung der Zweckbestimmung

	wiedergeben zu können. Das ist eine Aufgabe der Validierung. Bezeichnend ist auch, dass Art 17(1b) eine *„Entwurfsprüfung“* (*„design verification“*) aber keine *„Entwurfsvalidierung“* (*„design validation“*) enthält. Insgesamt fehlt damit eine konsequente Einführung des Begriffs Validierung (im klassischen Sinn, inkl. Abgrenzung gegenüber dem in der KI verwendeten Begriff im Sinne einer Optimierung / Adjustierung des Modells) und die für KI-Systeme damit verbundenen Anforderungen. Gegebenenfalls könnte auch auf weiterführende Verordnungen verwiesen werden, um Inkonsistenzen mit diesen zu vermeiden.
Im Artikel 10(3) fordert die KI-Verordnung *„Die Trainings-, Validierungs- und Testdatensätze müssen relevant, repräsentativ, fehlerfrei und vollständig sein.“*	Die Daten bei Machine Learning sind in den meisten Fällen nicht fehlerfrei, insbesondere dann, wenn sie auf Realweltdaten aufbauen. Das gilt sowohl für die Input- als auch für die Output-Daten (Gold Standard-Daten). Selbst bei menschlichen Bewertern (von Menschen durchgeführten Annotationen der Daten) gibt es in der Regel eine gewisse Fehlerrate (z.B. bei Klassifikationsaufgaben wie bei Bewertungen anhand von radiologischen Bildern oder auch Laborwerten bzgl. einer bestimmten Erkrankung). Zudem sind quantitative Daten, praktisch immer mit einem gewissen Messfehler behaftet, wenn sie durch Messsensorik aufgenommen oder auch durch einen menschlichen Beobachter definiert sind. Weiterhin werden die Daten nie vollständig sein. Wenn sie vollständig wären, würde kein spezieller KI-Algorithmus benötigt werden, um eine Aussage treffen zu müssen. Es gäbe ja immer einen passenden Referenzdatensatz. Machine Learning-Verfahren dienen ja gerade dazu, Generalisierungen anhand von repräsentativen, aber eben nicht vollständigen Daten vorzunehmen. Es bleibt damit unklar, wie Begriffe wie *„fehlerfrei“ und „vollständig*“ in der KI-Verordnung zu interpretieren sind.

Die KI Verordnung fordert in Art. 14(1): *„Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie während der Dauer der Verwendung des KI-Systems – auch mit geeigneten Werkzeugen einer Mensch-Maschine-Schnittstelle – von natürlichen Personen wirksam beaufsichtigt werden können.“* Weiterhin ist in Art. 14(2) angegeben: *„Die menschliche Aufsicht dient der Verhinderung oder Minimierung der Risiken für die Gesundheit, die Sicherheit oder die Grundrechte, die entstehen können, wenn ein Hochrisiko-KI-System bestimmungsgemäß oder unter im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird, insbesondere wenn solche Risiken trotz der Einhaltung anderer Anforderungen dieses Kapitels fortbestehen.“* und in Art. 14(4a), dass die Eigenschaft „die Fähigkeiten und Grenzen des Hochrisiko-KI-Systems vollständig zu verstehen und seinen Betrieb ordnungsgemäß zu überwachen, damit Anzeichen von Anomalien, Fehlfunktionen und unerwarteter Leistung so bald wie möglich erkannt und behoben werden können;“ gegeben sein muss.	Es bleibt unklar, was mit den Begriffen „wirksam“ und „menschliche Aufsicht“ gemeint ist. Wenn damit gemeint ist, dass ein Mensch in dem Sinne eine Überwachung durchführen können muss, dass er in Realzeit die Ergebnisse des Systems abgreifen, verstehen und darauf reagieren kann, dann erscheint das für viele KI-Systeme unrealistisch. Das würde z.B. Systeme ausschließen, bei denen im Regelbetrieb automatisiert bestimmte Steuerungen vorgenommen werden, z.B. automatisierte Adaption von Maschinenparametern in der Fertigung oder Konfiguration von Medizinprodukten. Wenn stattdessen eine „wirksame menschliche Überwachung“ auch damit gegeben ist, dass der Gesamt-Outcome des Systems z.B. in dem Sinne überwacht so werden kann, dass Anomalien ausreichend zuverlässig entdeckt werden können, dann wäre eine solche Forderung eher realistisch. Das bleibt jedoch unklar. Hinzu kommt, dass die *„Fähigkeiten und Grenzen des Hochrisiko-KI-Systems vollständig zu verstehen“* sein müssen, *„damit Anzeichen von Anomalien, Fehlfunktionen und unerwarteter Leistung so bald wie möglich erkannt und behoben werden können“*. Ein solch vollständiges Verständnis für die Leistungen eines Systems ist selbst bei Produkten ohne KI in der Regel nicht oder nur begrenzt gegeben. Bei der inneren Komplexität von vielen KI-Systemen erscheint diese Forderung um so mehr unrealistisch, wenn hier wirklich ein „vollständiges Verständnis“ gefordert ist. Dass ist eben auch bei vielen/den meisten anderen Produkten nicht wirklich gegeben. Erschwerend kommt dazu, dass eine „derartige Aufsicht“ gemäß Art. 14(2) dazu dient, Risiken zu reduzieren / zu minimieren, *„… insbesondere wenn solche Risiken trotz der Einhaltung anderer Anforderungen dieses Kapitels fortbestehen“*. Bei den meisten Produkten werden am Ende gewisse Risiken verbleiben. Dann ist gerade bei Medizinprodukten der Normalfall. Wichtig ist dabei eigentlich, dass keine inakzeptablen Risiken bestehen bleiben. Dass ist die Kernforderung einer Produktentwicklung in Bezug auf ein angemessenes Risikomanagement. Der Begriff „inakzeptabel“ fehlt jedoch hier.

	Dabei sollte, wie bereits an anderer Stelle angegeben, beim Risikomanagement verzichtet werden, die Risiken „*weitestmöglich*“ reduzieren zu müssen *(„as far as possible“*, siehe Art. 9(4a) und Kommentar dazu an anderer Position). Dann bliebe die Anforderung einer Reduktion nämlich bis zum vollen, aber nie zu erreichenden Minimum bestehen. Stattdessen sollte eine Anforderung gestellt werden, dass die *„menschliche Aufsicht“* (ebenso wie andere Risikominimierungsmaßnahmen) dazu dienen, die Risiken auf ein der Zweckbestimmung angemessenes Niveau zu bringen.
Art. 13(3e) fordert eine Beschreibung für *„die erwartete Lebensdauer des Hochrisiko-KI-Systems und alle erforderlichen Wartungs- und Pflegemaßnahmen zur Gewährleistung des ordnungsgemäßen Funktionierens dieses KI-Systems, auch in Bezug auf Software-Updates“*	Es bleibt an dieser Stelle unklar, was Begriffe wie *„Lebensdauer des Software-Systems“* und *„Software-Update“* umschreibt. Bei klassischen, zum Zeitpunkt eines Releases fixierten Software-Systems würde man hier den Code inkl. der dazugehörigen Daten verstehen. Bei KI-Systemen stellt aber auch die Datenbasis eine wichtige Komponente dar, die zudem für die Leistungsfähigkeit des Systems maßgeblich ist. Stellen Änderungen der Datenbasis bereits ein Software-Update dar, wenn Software-Systeme einen fixen Stand haben bzw. auch wenn es sich um kontinuierlich lernende Systeme handelt? Wie muss ein Update des Datenbestandes dokumentiert werden, wenn es Updates der lokalen Datenbasis beim Benutzer mit eingeschlossen sind?
Art. 28(1c) sagt, dass u.a. Benutzer zu einem Anbieter werden und damit Pflichten wie Sicherstellung der Anforderungen an KI-Systeme, Qualitätsmanagementsystem, … haben, *„wenn sie eine wesentliche Änderung an dem Hochrisiko-KI-System vornehmen.“*	Es bleibt unklar, was eine wesentliche Änderung ist. Ist z.B. eine Erweiterung des Trainingsdatenbestandes, der eine Änderung der Genauigkeit der Vorhersagen eines KI-Systems, z.B. in Form Adaptierung des Systems an die Gegebenheiten eines Betriebs, bereits eine wesentliche Änderung? Eine generelle Auferlegung all dieser Pflichten an den Benutzer erscheint in diesem Zusammenhang unverhältnismäßig.
In Erwägungsgrund (50) wird angegeben: „Ein fehlender Schutz vor diesen Risiken könnte die Sicherheit beeinträchtigen oder sich negativ auf die Grundrechte auswirken, wenn das KI-System beispielsweise	Während im Erwägungsgrund das Problem der Entstehung von Bias in den Resultaten angesprochen wird, sind in der Verordnung in Bezug auf die Bias-Problematik im Wesentlichen nur Untersuchungen der Input-Daten sowie der Effekt des Automatisierungs-Bias bei kontinuierlich

falsche Entscheidungen trifft oder falsche oder verzerrte Ergebnisse hervorbringt.“ Anforderungen bzgl. Bias-Effekten sind zu finden in Art. 10(2), dass in Bezug auf die verwendeten Trainings-, Test- und Validierungsdaten *„eine Beobachtung, Erkennung und Korrektur im Hinblick auf mögliche Verzerrungen (Bias)“* und gemäß Art. 10(5) eine *„Erkennung und Korrektur von Verzerrungen“* (*„bias monitoring, detection and correction“*) bzgl. der Daten durchzuführen ist. In Bezug auf kontinuierlich lernende Systeme soll zudem überprüft werden, ob eine *„mögliche Neigung zu einem automatischen oder übermäßigen Vertrauen in das von einem Hochrisiko-KI-System hervorgebrachte Ergebnis („Automatisierungsbias“)“* vorliegt (siehe Art. 14(4b)), und dass für diese Systeme *„auf möglicherweise verzerrte Ergebnisse, die durch eine Verwendung vorheriger Ergebnisse als Eingabedaten für den künftigen Betrieb entstehen („Rückkopplungsschleifen“), angemessen mit geeigneten Risikominderungsmaßnahmen eingegangen wird“*.	lernenden Systemen angegeben. Eine Adressierung von Bias-Effekten in den Resultaten eines KI-Systems fehlen.
Der Artikel 64 der KI-Verordnung verlangt von den Herstellern den Behörden einen vollständigen Remote-Zugriff zu den Trainings-, Validierungs- und Testdaten zu verschaffen, sogar durch eine API.	Vertrauliche Patientendaten über einen Remote-Zugriff zugreifbar zu machen, steht in einem gewissen Maße im Konflikt mit der gesetzlichen Forderung nach Data Protection by Design. Gesundheitsdaten zählen zur besonders schützenswerten Kategorie personenbezogener Daten. Eine externe API zu den Trainingsdaten zu entwickeln und mit entsprechenden Sicherheitsmechanismen bereitzustellen, bedeutet für die Hersteller einen erheblichen Mehraufwand und erscheint unverhältnismäßig. Zudem entsteht durch derartige Backdoors immer eine gewisse Sicherheitsgefährdung bzgl. des Zugangs zu persönlichen und vertrauenswürdigen Daten. Bei anderen, oft sogar kritischeren Daten und Informationen zum Design und zur Produktion von Produkten (z.B. Source-Code oder CAD-Zeichnungen) würde niemand verlangen, dass die Hersteller den Behörden einen Remote-Zugriff gewähren müssen.