

Empfehlungen zum Datenschutz Soziale Roboter

Auftakt 31.01. 2023 /
Prot. 1, 23

2 Anhänge

AI Act

Beispielfälle

Folgende Themen wurden angesprochen:

Zulässigkeitsvoraussetzungen zur Verarbeitung von Daten, die Cloud - Nutzung und Anonymisierung, TOM.

Die folgenden Erläuterungen dienen zum besseren Verständnis und dem Zweck erste Zwischenergebnisse festzuhalten. Es wurde die aktuelle Rechtslage berücksichtigt. Auf die Entwicklungen zum EU AI Act wurde hingewiesen.

I) Rechtliche Grundlagen

Die einschlägigen Bestimmungen zum Datenschutz finden sich derzeit insbesondere in der Datenschutzgrundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG). Spezialregelungen gelten für Sozialdaten nach dem SGB I §35 und X § 67 ff und für Steuerdaten nach §29ff AO.

Als wesentliche verlässliche Quellen für die einheitliche Anwendungen des Rechts wurde insbesondere auf die Erwägungsgründe (sog. „Softlaw“) hingewiesen und auf das Standard Datenschutzmodel (SDM) der Bundes- und Landesaufsichtsbehörden.

Im Moment bereitet die EU einen sog. AI Act als Verordnung mit umfangreichen Anlagen vor. Die VO soll spätestens 2024 in Kraft treten.

Hierin wird für KI eine spezialgesetzliche Regelung geschaffen, die zu den Bestimmungen der DSGVO hinzutritt. Je nach Risikoeinschätzung werden unterschiedliche Notifikationen gefordert.

Link:

https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_1&format=PDF

https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_2&format=PDF

Auszüge aus den Entwürfen befinden sich im Anhang

Spezialfall KI in der DSGVO

Für Verarbeitungen mit Hilfe von KI wählt die DSGVO den Begriff der „automatisierten Entscheidung“. Hierzu enthält Art. 22 DSGVO spezielle Regelungen, die sich allerdings weitgehend als gesteigerte Form der automatisierten Verarbeitung darstellen. Art. 22 DSGVO beinhaltet 3 grundlegende Aussagen:

- Die Regelung gilt nur, soweit die Entscheidung ausschließlich automatisiert, d.h. ohne menschliches Zutun erfolgt.
- Der Mensch soll grundsätzlich nicht Gegenstand einer maschinellen Entscheidung sein.
- Es muss eine explizite Interventionsmöglichkeit bestehen.

Der Begriff der automatisierten Entscheidung findet sich an unterschiedlichen Stellen der DSGVO zur Wahrung der Rechte der Betroffenen z.B. Auskunftsrechte, Transparenz, Risikobewertung.

Für das vorliegende Projekt RuhrBots wird es daher wesentlich darauf ankommen, ob es sich um eine Verarbeitung herkömmlicher Art, eine niederschwellige „schwache“ KI, eine selbstlernende KI oder um eine eigenständige automatisierte Entscheidung oder um eine Mischform handelt. Bei Mischformen sollte den strengeren Anforderungen der Vorzug gegeben werden.

Für die Entwicklung von KI Systemen sind unbestritten große Datenmengen erforderlich. Damit ergibt sich das Problem, dass bereits für die Verwendung von Daten in der Lernphase bereits Daten erhoben und verarbeitet werden müssen. Diese dienen aber nicht der Anwendung im Betrieb, sondern der Entstehung der Anwendung.

Lernphase und Echtdate

Bei der Entwicklung einer KI- Anwendung wird zwischen der Lernphase und der Echtphase (Scharfschaltung) unterschieden. Hier muss ganz grundsätzlich entschieden werden, ob mit **Echtdate**n gearbeitet werden soll. Es muss daher entschieden werden, woher diese Daten kommen und auf welcher Grundlage sie erhoben werden oder ob man mit anonymisierten Daten arbeiten kann oder nur mit sog. fiktionalen Spieldaten.

Bei der Verwendung fremder Daten aus anderen Erhebungszwecken muss stets die Änderung der Nutzung erlaubt sein. Es wird aus diesem Grund auch der Ansatz des föderalen Lernens verfolgt. Daten werden verarbeitet, analysiert und die Ergebnisse bzw. die anonymisierten Daten bereitgestellt. Die Diskussion hält an.

Der AI Act EU schlägt hierfür die Einrichtung des Reallabors vor, sh. Anhang

Die Verarbeitung von Daten mit Personenbezug ist grundsätzlich verboten, es sei denn, es liegt ein Erlaubnistatbestand vor.

- 1) **Verarbeitungen** sind danach alle typischen Schritte im Umgang mit diesen Daten, nicht abschließend aber weitgehend erschöpfend in Art. 4 Nr. 2 DSGVO geregelt. Zu nennen sind insbes. das Erheben, Speichern, Auslesen, Verknüpfen und Übermitteln, u.a.m.

Zu beachten ist dabei, dass im Vordergrund zwar die Verarbeitung von Daten der Nutzer:innen der KI steht, jedoch stets auch die Verarbeitung von Daten der Beschäftigten im Umgang mit der KI hinzutritt. Es werden Befugnisse im Umgang mit der KI zu verwalten sein.

- 2) Die Datenverarbeitung kann gestattet sein auf der Grundlage einer **Einwilligung** des Betroffenen nach Art. 6 Abs 1, lit a DSGVO. Die Einwilligung muss den Anforderungen des Art. 7 DSGVO genügen (Information, verständlich, eindeutig, freiwillig).

Für die Einwilligung von Kindern, die Einwilligung in die Verarbeitung von besonders sensiblen Daten (nach Art. 9 DSGVO z.B. Gesundheitsdaten, etwa wenn ein behinderter Mensch die Bücherei nutzt), und auch bei der automatisierten Entscheidung muss sich die Einwilligung spezifisch auf diese Aspekte beziehen.

Die Verarbeitung von **Daten von Beschäftigten** ist spezialgesetzlich in § 26 BDSG geregelt. Soweit es sich um erforderliche Verarbeitung von Beschäftigtendaten zur Erfüllung des Arbeitsvertrages handelt, ist keine gesonderte Einwilligung erforderlich. Würden sich aber z.B. Beschäftigte der Fakultät für die Trainingsphase bereit erklären, ihre Daten nutzen zu lassen, müssten Einwilligungen eingeholt werden.

- 3) Als Rechtsgrundlage kommt auch das Erfordernis einer **Vertragserfüllung** in Betracht (z.B. für die Kundschaft einer Bibliothek). Hier muss aber auch von Seiten des Vertragspartners eine **Datenverarbeitung bekannt und gewünscht sein**. Bei Angeboten der öffentlichen Verwaltung, z.B. Bibliotheksdienst kommt es auf die Ausgestaltung der Nutzungsbedingungen an. Der Vertrag kann auch unentgeltliche Leistungen umfassen.

Die Zweckbestimmung der Datenverarbeitung ist auch hier unerlässlich, sie wird z.B. durch AGB und eine Datenschutzerklärung verankert und findet sich auch in zwingenden Dokumentationen z.B. im Datenschutzkonzept.

- 4) Besonders im Bereich der öffentlichen Verwaltung kommt die Zulässigkeit der Verarbeitung auf der Grundlage einer **Rechtsvorschrift nach** Art. 6 Abs.3 DSGVO in Betracht. Eine solche Rechtsvorschrift könnte auch eine Satzung auf der Grundlage der gemeindlichen Selbstverwaltung sein. In einer Satzung zur Nutzung gemeindlicher Einrichtungen oder einer Bücherei könnte diese Bestimmung Eingang finden. Es könnte also auch die Ergänzung (!) einer bestehenden gemeindlichen/städtischen Satzung genügen.

Die Bestimmung muss dabei die Mindestanforderungen des Abs. 3 erfüllen: Zweckbestimmung in öffentlichem Interesse, Speicherdauer. Die Vorschrift kann dabei so allgemein wie nötig, aber auch so spezifisch zielgerichtet wie möglich ausgestaltet sein.

- 5) Insbesondere für die Verarbeitung von Daten besonders sensibler Daten zu **Forschungszwecken** hält Art. 9 Abs. 2 lit j DSGVO eine spezielle Ermächtigung bereit, die in § 27 Bundesdatenschutzgesetz (BDSG) eine spezielle Ausformung erfährt.

Diese Rechtsgrundlage ist zwar auf den ersten Blick für die KI Entwicklung verlockend, soweit es um die Entwicklung einer neuen Technik geht, also um eine Forschung, doch unterliegt sie außerordentlich hohen Anforderungen in Bezug auf Abwägung, Erforderlichkeit und Sicherungsmaßnahmen, vergl. §22 BDSG.

Für die Praxisanwendung ist diese Rechtsgrundlage nicht anwendbar, allerdings könnte sie relevant werden, wenn es um die Umsetzung der Lernphase geht und dort z.B. um den Einsatz von Echtdaten.

Bewertung

Für Verarbeitungen der öffentlichen Verwaltung ist im Regelfall die Rechtsgrundlage in Form eines Gesetzes oder einer niedrigeren Rechtsvorschrift das angezeigte Mittel. Da es sich im Bereich der Museen oder Bibliotheken aber um eine öffentliche Leistungsverwaltung handelt, die auch im Gewand des Privatrechts in Erscheinung treten kann, kommt hier auch die Rechtsgrundlage im Sinne der Vertragserfüllung in Betracht. Dies hat 3 wesentliche Vorteile:

- Die Anforderungen sind niedriger als bei der Einwilligung
- Die Regelung kommt auch bei automatisierten Entscheidungen nach Art.22 zur Anwendung.
- Die Regelung gilt bereits bei der Vertragsanbahnung—müsste dazu aber bereits in der Begrüßungsphase auf die Verarbeitung hinweisen

Z.B. „guten Tag, ich bin der ROBI, wenn Sie sich für die Ausleihe interessieren und die Bücherei nutzen wollen, kann ich Ihnen gerne helfen. In diesem Fall muss ich Ihre Daten aber auch elektronisch erfassen und verarbeiten. Wenn Sie meinen Dienst möchten, erhalten Sie weitere Informationen über den Umgang mit Ihren Daten.

Möchten Sie nun meine Dienste in Anspruch nehmen? “

Das Beispiel würde beide Aspekte (Vertrag und Einwilligung) miteinander verknüpfen. In der Folge muss die Frage geklärt werden, auf welchem Weg die weiteren Informationen übermittelt werden (denkbar z.B. bei der Ausstellung des Nutzerausweises).

Fundstellen zu Ziff II)

Erwägungsgründe 40- 45, 49, 51, 58

Auernhammer, Kramer in Kommentar zur DSGVO / BDSG Art. 6, Rz 97

III) Vorkehrungen zum Schutz von Persönlichkeitsrechten

Je tiefer die Verarbeitung in die Rechte der Betroffenen eingreift, desto ausgeprägter müssen die Schutzvorkehrungen sein. Es wird dabei zwischen besonders **sensiblen Daten**

(Gesundheit Geschlecht, Religion Kinder) und **sensiblen Verarbeitungen** (Biometrie, Profiling, Scoring) unterschieden.

Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung biometrischer Daten – als Daten mit besonderer Sensibilität – grundsätzlich verboten.

Absatz 2 nennt eine Reihe von Ausnahmen. Für die Robotik kommt nur die Einwilligung nach Abs.2 lit a in Betracht. Sie muss spezifisch auf den Zweck ausgerichtet sein. Diese Bestimmung ist im Falle einer KI-Anwendung stets gemeinsam mit Art. 22 Abs.4 DSGVO umzusetzen, indem ausgewählte Schutzvorkehrungen getroffen werden müssen.

Die Vertragserfüllung kommt für die Anwendung von Biometrie nicht in Betracht, hier hilft nur die qualifizierte Einwilligung (vergl. Aurnhammer Art.9 DSGVO, Rz 19, Erwgr. 58,60).

TOM

Schutzvorkehrungen werden in der DSGVO als „technisch organisatorische Maßnahmen“ (sog. TOM) eingefordert, hierzu zählen z.B. kurze Lösungsintervalle, Anonymisierung, eingeschränkte Verarbeitung durch Verschieben in ein Sperrregister, Übertragung auf Sicherungskopien, Zugangsbeschränkungen für Mitarbeiter durch Rollenbefugnisse, gesonderte Ablage (Sharepoint), Kontrollwerkzeuge für die Aufsicht durch Lesebefugnis zu Zugriffsprotokollen für den DSB, elektronisch verankerte Ausdruckuntersagung, Sperrung des USB-Zugangs, Intervention des Betroffenen, Erläuterung der Logik in der Datenschutzerklärung, Verwendung der KI Ergebnisse nur in Verbindung mit vorangehender menschlicher Überprüfung, Schulungen, Verfahrensanweisungen, Verbot der Nutzungsänderung usw.

Beispiele einer verbotenen Nutzung von Bibliotheksdiensten, sh. Anhang

IV) Cloud – Nutzung

Eine Cloud verbindet mehrere große Server zu einem Verbund, um mächtige Speicherkapazitäten bereitzustellen. Besonders bei Big Data kann nur mehr schwer nachvollzogen werden in welchen Servern abgelegt wird, wer Zugang zu den Daten hat und zu welchen Zwecken Daten ausgetauscht werden.

Die Cloudablage hat deshalb insbesondere bei sensiblen Daten große Bedenken ausgelöst. Besondere Schwierigkeiten ergeben sich aber auch aus dem Umstand, dass sich die verwendeten Server im Zugriffsbereich der DSGVO also bei EU-Mitgliedern befinden müssen,

um einen Mindeststandard zu garantieren, bei dem insbesondere die Sanktions- und Überwachungsmechanismen zu gewährleisten sind.

Es war deshalb ein Gebot der technischen Entwicklung, sichere Cloudumgebungen zu bilden. Hierzu wurden entweder eigene Server zusammengeführt, zertifizierte Rechenzentren (ITZ BUND) eingebunden oder zertifizierte private Anbieter genutzt.

Ein weiteres, aber lösbares Problem, das bei Datenübermittlung und Datenabruf ganz generell auftaucht, ist die Frage nach einer sicheren Übermittlungsweise. Daten dürfen nicht verloren gehen, in falsche Hände geraten oder abgegriffen werden. Dies wird durch eine Kombination an Mitarbeiterschulung, Anweisung und Technikgestaltung erreicht. Diese Fragen berühren weniger nur den Datenschutz als vielmehr auch die Datensicherheit:

- Verteiler sind zu prüfen,
- es wird eine Ende-zu-Ende Verschlüsselung
- mittels sog. VPN Tunnel über die Provider eingerichtet
- und ein Vertrag zur **Auftragsdatenverarbeitung nach Art. 28 DSGVO** geschlossen.

Fundstellen zu Ziff III

Art. 28 DSGVO, SDM S.42

<https://www.cloudcomputing-insider.de/die-10-groessten-gefahren-beim-einsatz-von-cloud-infrastrukturen-a-517146/>

<https://hochschulcloud.nrw/de/projekt/>

https://www.it-planungsrat.de/fileadmin/it-planungsrat/der-it-planungsrat/fachkongress/fachkongress_2021/Tag_1_Cloud_Computing_in_NRW.pdf

Landescloud NRW: <https://www.landes.cloud/>

Clemens, K. / Steinert, C. (2022): Roboter in der Stadt Bergheim. In: Andreas Gourmelon (Hrsg.): Digitalisierung und deren Folgen für das Personalmanagement, rehm Verlag, S.36.

V) Anonymisierung

Das Wesen der Anonymisierung besteht darin, den Personenbezug von Daten aufzuheben. Mit dem Einsatz von Anonymisierungstechniken soll erreicht werden, dass die betroffene Person nicht mehr identifiziert werden kann. Brauchbare Anonymisierung versucht gleichzeitig aber, den maximalen Erklärungsgehalt von Daten zu bewahren. Nutzen und Werthaltigkeit von Daten auf der einen, Schutz der Menschen auf der anderen Seite.

Wann aber eine Anonymisierung als hinreichend angesehen werden kann, darüber gibt die DSGVO keine abschließende Auskunft. Die Kommentierungen beziehen den Aufwand der Re-Identifizierung in die Bewertung mit ein. Ist der Aufwand wirtschaftlich groß, die Daten im Verhältnis nicht herausgehoben sensibel, kann die Anonymisierung ausreichend sein.

Der BfDI hat im Rahmen einer öffentlichen Konsultation im Juni 2020 zur Frage der Anonymisierung folgende drei Ergebnisse herausgearbeitet:

1. Jede Anonymisierung stellt eine Verarbeitung personenbezogener Daten dar und bedarf deshalb einer Rechtsgrundlage.
2. Die Verpflichtung zur Löschung von personenbezogenen Daten ist durch Anonymisierung erfüllbar.
3. Im Rahmen der Transparenzpflichten haben die Verantwortlichen den Betroffenen die Zwecke und die Rechtsgrundlage der Anonymisierung mitzuteilen.

Auch auf europäischer Ebene wird derzeit an solchen neuen Leitlinien für Anonymisierung gearbeitet. Es handelt sich dabei um sog. genehmigte Verhaltensregeln nach Art. 40 DSGVO, die quasi mit einer Zertifizierung (Art.42 DSGVO) gleichkommen.

Man kann sich der Frage einer tauglichen Anonymisierung auch von der Seite des „Misserfolgs“ her nähern. Hierzu wurden 3 Kriterien herausgearbeitet:

1. „Singling Out“ meint das Vorhandensein von eindeutigen Daten, die zu einer individuellen Person gehören.
2. „Linkage“ beschreibt die Möglichkeit, einen Eintrag mit einem zur gleichen Person gehörenden weiteren Eintrag aus einem anderen Datensatz zu verbinden.
3. „Inference“ ist die Möglichkeit, aus den Daten Informationen über eine Person herzuleiten, beispielsweise die Tatsache, dass personenbezogenen Daten dieser Person in die Anonymisierung mit eingeflossen sind.

Zur Verwendung in der Lernphase könnte es erforderlich werden, auf Echtdaten zurückzugreifen. Durch deren Anonymisierung könnten dabei aber Funktionalitäten fehlgeleitet werden. Um dies zu verhindern, könnten personalisierte Daten durch Fakedaten **ersetzt werden**.

Fundstellen zu Ziff V

Art. Erwgr. 26 Satz 4 u.5

Auernhammer DSGVO Art.4 Rz. 72-74

Vortrag des BfDI Dr.Kelber vom 07.12. 2022 : „Die Anonymisierung im Datenschutzrecht“

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Reden_Gastbeitr%C3%A4ge/2022/Anonymisierung-im-DS-recht.pdf?__blob=publicationFile&v=2

Els Stellungnahme zur Konsultation des BfDI v. 29.06. 22

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Stellungnahmen/Dr-Els.html

V) Ausblick

In den folgenden Sitzungen sollte über die Frage der datenschutzrechtlichen Verantwortung während der Entwicklung und der Echtnutzung nachgedacht werden.

Zudem sollte bei einer Vorbereitung der Nutzung von Echtdateien die Landesdatenschutzaufsicht konsultiert / informiert werden.

VI) Herausforderung

Technikgestaltung

Ein Forschungsprojekt sollte in Bezug auf den Schutz der Rechte von Betroffenen und der Implementierung technischen Fortschritts erkennbar neue Wege ausloten.

Die gesetzlichen Grundlagen fordern genau dies auch ein (vergl. Art. 25 DSGVO und Erwgr. 78).

Privacy by design und Privacy by default verlangen, dass bereits in der Phase der Verfahrensentwicklung daran gedacht wird diese Forderungen zu erfüllen.

Beim Kauf von „vorgefertigten Produkten“ steht natürlich im Vordergrund, welche Funktionen verwirklicht werden können und wie die Erscheinung des Roboters Akzeptanzhürden nimmt, gleichwohl sollte darauf geachtet werden, welche Konfigurationen in Bezug auf Datenschutz bereits vorgesehen bzw. noch möglich sind.

Stand der Technik

Die DSGVO verlangt, dass bei der Ausgestaltung zumindest der Stand der Technik berücksichtigt wird. Das bedeutet, dass aktuelle, eingeführte Technik zur Anwendung kommen soll. Im Regelfall müssen also nicht neue Technologien aufwändig entwickelt werden.

Ob dies aber auch für die Entwicklung innovativer Robotertechnik im Rahmen eines Forschungsprojektes gilt, darf zumindest auf den Prüfstand.

Es erscheint deshalb sinnvoll bislang unbegangene Wege einzuschlagen, so kommt im Falle der Cloudnutzung für die Wiedererkennung von Biometriedaten auch die Nutzung der Präsenz-Detektion in Betracht. Dies würde eine Cloudnutzung vermeiden, die Daten bleiben im Begrüßungsraum.

Auch die speziell bei KI-Einsatz als von herausragender Bedeutung erkannte Transparenz und Aufklärung (z.B. bei der Einwilligung) sollte versuchen neue innovative Wege zu gehen. So stellt es durchaus eine Herausforderung dar, die in § 22 Abs. 2 BDSG geforderten Kriterien lesbar und übersichtlich zu „verpacken“. Eine Erwähnung der Information in ausufernden Datenschutzerklärungen und Beiblättern oder AGB erscheint jedenfalls nicht als geeignetes

Anlage1 zu einschlägigen Texten des AI Act EU:

Öffentliche Anhörung des Ausschusses für Digitales im Bundestag Stellungnahme zum Fragenkatalog „EU-Verordnung zu Künstlicher Intelligenz unter Einbeziehung von Wettbewerbsfähigkeit im Bereich Künstliche Intelligenz und Blockchain-Technologie“:

S.8.....Politisch wird in diesem Kontext, zunächst in den Bundesländern Hessen, Nordrhein-Westfalen und Berlin, das Konzept der AI Quality & Testing Hubs vorangetrieben, welche der TÜV-Verband für ein geeignetes Instrument hält. Übergeordnetes Ziel ist es, die Grundlagen für qualitativ hochwertige KI-Anwendungen zu legen, die technisch sicher und ethisch unbedenklich sind. Dies erfolgt, indem Akteur:innen und Verfahren zusammengebracht werden, die für das Bewerten und das Management der KI-Systeme notwendig sind. Angefangen von der Auflistung von Forschungsständen über den Zugang und den Aufbau von Trainings Datensätzen sowie Simulationsumgebungen mit standardisierten Interfaces, bis hin zum Trainings- und Kompetenzerwerb für Anbietende und Anwendende/Betreibende von KI-Systemen.

Auszüge aus dem Entwurf zu KI EU VO

36. „biometrisches Fernidentifizierungssystem“

ein KI-System, das dem Zweck dient, natürliche Personen aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren, ohne, dass der/die Nutzende des KI-Systems vorher weiß, ob die Person anwesend sein wird und identifiziert werden kann; 37. „biometrisches Echtzeit-Fernidentifizierungssystem“ ist ein biometrisches Fernidentifizierungssystem, bei dem die Erfassung biometrischer Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen; zur Vermeidung einer Umgehung der Vorschriften, umfasst dies nicht nur die sofortige Identifizierung, sondern auch eine Identifizierung mit begrenzten kurzen Verzögerungen; 38. „System zur nachträglichen biometrischen Fernidentifizierung“ ist ein biometrisches Fernidentifizierungssystem, das kein biometrisches Echtzeit-Fernidentifizierungssystem ist;

Artikel 9 Risikomanagementsystem

- (1) Für Hochrisiko-KI-Systeme wird ein Risikomanagementsystem eingerichtet, angewandt, dokumentiert und aufrechterhalten. (2) Das Risikomanagementsystem versteht sich als ein kontinuierlicher iterativer Prozess während des gesamten Lebenszyklus eines KI-Systems, der eine regelmäßige systematische Aktualisierung erfordert. Es umfasst folgende Schritte: a) Ermittlung und Analyse der bekannten und vorhersehbaren Risiken, die von jedem Hochrisiko-KI-System ausgehen; b) Abschätzung und Bewertung der Risiken, die entstehen können, wenn das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird;

Artikel 52 Transparenzpflichten für bestimmte KI-Systeme

- (1) Die Anbieter:innen stellen sicher, dass KI-Systeme, die für die Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden, dass natürlichen Personen mitgeteilt wird, dass sie es mit einem KI-System zu tun haben, es sei denn, dies ist aufgrund der Umstände und des Kontexts der Nutzung offensichtlich. Diese Vorgabe gilt nicht für

gesetzlich zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten zugelassene KI-Systeme, es sei denn, diese Systeme stehen der Öffentlichkeit zur Anzeige einer Straftat zur Verfügung. (2) Die Verwender:innen eines Emotionserkennungssystems oder eines Systems zur biometrischen Kategorisierung informieren die davon betroffenen natürlichen Personen über den Betrieb des Systems.

Artikel 53 KI-Reallabore

- (1) KI-Reallabore, die von den zuständigen Behörden eines oder mehrerer Mitgliedstaaten oder vom Europäischen Datenschutzbeauftragten eingerichtet werden, bieten eine kontrollierte Umgebung, um die Entwicklung, Erprobung und Validierung innovativer KI-Systeme für einen begrenzten Zeitraum vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme nach einem spezifischen Plan zu erleichtern. Dies geschieht unter direkter Aufsicht und Anleitung der zuständigen Behörden, um die Einhaltung der Anforderungen dieser Verordnung und gegebenenfalls anderer Rechtsvorschriften der Union und der Mitgliedstaaten, die innerhalb des Reallabors beaufsichtigt wird, sicherzustellen. (2) Soweit die innovativen KI-Systeme personenbezogene Daten verarbeiten oder anderweitig der Aufsicht anderer nationaler Behörden oder zuständiger Behörden unterstehen, die den Zugang zu Daten gewähren oder unterstützen, sorgen die Mitgliedstaaten dafür, dass die nationalen Datenschutzbehörden und diese anderen nationalen Behörden in den Betrieb des KI-Reallabors einbezogen werden.

Artikel 54 Weiterverarbeitung personenbezogener Daten zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse im KI-Reallabor

- (1) Im KI-Reallabor dürfen personenbezogene Daten, die rechtmäßig für andere Zwecke erhoben wurden, zur Entwicklung und Erprobung bestimmter innovativer KI-Systeme im Reallabor unter folgenden Bedingungen verarbeitet werden: a) die innovativen KI-Systeme werden entwickelt, um ein erhebliches öffentliches Interesse in einem oder mehreren der folgenden Bereiche zu wahren:

..., soweit diese Anforderungen durch die Verarbeitung anonymisierter, synthetischer oder sonstiger nicht personenbezogener Daten nicht wirksam erfüllt werden können;

- d) personenbezogene Daten, die im Rahmen des Reallabors verarbeitet werden sollen, befinden sich in einer funktional getrennten, isolierten und geschützten Datenverarbeitungsumgebung unter der Kontrolle der Beteiligten, und nur befugte Personen haben Zugriff auf diese Daten;

Artikel 59 Benennung der zuständigen nationalen Behörden

- (1) Um die Anwendung und Durchführung dieser Verordnung sicherzustellen, werden von jedem Mitgliedstaat zuständige nationale Behörden eingerichtet oder benannt. Die notifizierenden Behörden werden so organisiert, dass bei der Ausübung ihrer Tätigkeiten und der Wahrnehmung ihrer Aufgaben Objektivität und Unparteilichkeit gewahrt sind. (2) Jeder Mitgliedstaat benennt aus der Reihe der zuständigen nationalen Behörden eine nationale Aufsichtsbehörde. Die nationale Aufsichtsbehörde fungiert als notifizierende Behörde und als Marktüberwachungsbehörde, es sei denn, der Mitgliedstaat hat organisatorische und administrative Gründe, um mehr als eine Behörde zu benennen.

ANHANG III HOCHRISIKO-KI-SYSTEME GEMÄß ARTIKEL 6 ABSATZ 2 Als Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2 gelten die in folgenden Bereichen aufgeführten KI-Systeme: 1. Biometrische Identifizierung und Kategorisierung natürlicher Personen: a) KI-Systeme, die bestimmungsgemäß für die biometrische Echtzeit Fernidentifizierung und nachträgliche biometrische Fernidentifizierung natürlicher Personen verwendet werden sollen;

ANHANG IV TECHNISCHE DOKUMENTATION GEMÄß ARTIKEL 11 ABSATZ 1

Die in Artikel 11 Absatz 1 genannte technische Dokumentation muss mindestens die folgenden Informationen enthalten, soweit sie für das betreffende KI-System von Belang sind:

1. Allgemeine Beschreibung des KI-Systems einschließlich:

- a) Zweckbestimmung, das System entwickelnde Person(en), Datum und Version des Systems;
- b) gegebenenfalls Interaktion oder Verwendung des KI-Systems mit Hardware oder Software, die nicht Teil des KI-Systems selbst sind;
- c) Versionen der betreffenden Software oder Firmware und etwaige Anforderungen in Bezug auf die Aktualisierung der Versionen;
- d) Beschreibung aller Formen, in denen das KI-System in Verkehr gebracht oder in Betrieb genommen wird;
- e) Beschreibung der Hardware, auf der das KI-System betrieben werden soll;
- f) falls das KI-System Bestandteil von Produkten ist: Fotografien oder Abbildungen, die äußere Merkmale, Kennzeichnungen und den inneren Aufbau dieser Produkte zeigen;
- g) Gebrauchsanweisungen für d

Anlage 2 Beispielfälle Bibliotheksdienste

Fall 1

Ein Fachverlag erstellt mittels KI Examensklausuren für Übungszwecke für Lehrer, Rechtspfleger und Juristen. KI bezieht dabei die neusten Entwicklungen der Methodik und der Rechtsprechung ein.

Die Daten der Nutzer:innen (ggfls. mit Ergebnissen der Benotung) werden absichtlich oder versehentlich an eine private Krankenversicherung weitergeleitet oder es wird Zugang verschafft. Dort werden sie zu Werbezwecken herangezogen. Den Nutzer:innen wird ein Versicherungsangebot unterbreitet.

Fall 2

Auffälligkeiten der Nutzer:innen in Bezug auf Behandlung der Bücher, Verlässlichkeit und Zahlungsmoral werden erfasst und mittels KI ausgewertet. Hierbei ergeben sich aus Massedaten algorithmisch gefilterte Auffälligkeiten. Schließlich erzeugt das System einen Score-Wert, der auf künftige Vertragsgestaltungen (z.B. Modalitäten bei der Ausleihe) Einfluss nehmen kann.