4/2023
73 – 96

EuGH
Österreichische Post
Thomas Schweiger

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Künstliche Intelligenz und Datenschutz

Europa setzt Maßstäbe im KI-Recht

Interview mit Martin Selmayr, EK

DGA, DMA, DSA, DA, AI Act, EHDS – ein Überblick (Teil 2)

Rainer Knyrim und Lena Urban

Was ist der EDHS?

Michael Löffler und Markus Kastelitz

AI Act: Das Ende der Innovation oder Gefahr für den Datenschutz?

Tünde Fülöp

ChatGPT und Mitarbeiter:innen – ein Risiko?

André Rohrleitner

Checkliste: KI und Datenschutz

Hans-Jürgen Pollirer

ISSN 2313-5409

dako.manz.at

MANZ

Hans-Jürgen Pollirer
Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH

Checkliste Künstliche Intelligenz und Datenschutz

ChatGPT; Umsetzungsfristen. Die Checkliste unterstützt Unternehmen, die in ihren automationsunterstützten Verfahren KI-Systeme direkt oder über Schnittstellen einsetzen, ihre Anwendungen auf die Einhaltung der Bestimmungen der DSGVO zu prüfen. Während bei der DSGVO der Schutz der personenbezogenen Daten im Vordergrund steht, gibt die KI-VO den Rahmen für den generellen Umgang mit Daten vor.

Einleitung

Mit ChatGPT geriet Ende 2022 erstmals eine KI (Künstliche Intelligenz)-Anwendung in das Zentrum des öffentlichen Interesses. KI-Anwendungen gibt es schon seit vielen Jahren, allerdings sind wir ihnen bisher nur selten bewusst begegnet.

Versuchen wir einmal, was ChatGPT selbst zur Entwicklung von KI, ihren Anwendungsbereichen und dem Spannungsverhältnis zwischen geltendem Datenschutzrecht und KI-Anwendungen einfällt. Die folgende **Aufgabe** wurde am 25. 5. 2023 an **ChatGPT gestellt**:

> Schreibe einen Text, ca 2 Seiten lang, über die Anfänge und Entwicklung der Künstlichen Intelligenz. Gehe hierbei auf Pioniere in der Entwicklung ein und erläutere genau die Anwendungsbereiche, in denen heute Künstliche Intelligenz eingesetzt wird. Gehe auf die problematischen Herausforderungen in der Anwendung Künstlicher Intelligenz ein und betone das Spannungsverhältnis zum geltenden Datenschutzrecht. Schreibe in Fachsprache und gutem Deutsch.

Die Anfänge der Künstlichen Intelligenz (KI) reichen zurück in die 1950er Jahre, als Forscher begannen, Maschinen zu entwickeln, die in der Lage waren, menschenähnliches Denken und Lernen nachzubilden. Einer der Pioniere auf diesem Gebiet war der amerikanische Mathematiker und Informatiker John McCarthy, der den Begriff „Künstliche Intelligenz" prägte und maßgeblich zur Entwicklung der KI beitrug.

In den folgenden Jahrzehnten hat sich die Künstliche Intelligenz stark weiterentwickelt. Frühe KI-Systeme waren hauptsächlich auf Expertensysteme beschränkt, die spezifisches Fachwissen in Form von Regeln und Heuristiken nutzten. Mit dem Aufkommen des maschinellen Lernens und der Entwicklung leistungsfähiger Algorithmen hat sich die KI jedoch weiterentwickelt und kann nun komplexere Aufgaben bewältigen.

Heute finden wir KI-Anwendungen in einer Vielzahl von Bereichen. In der Medizin werden KI-Modelle eingesetzt, um Diagnosen zu stellen, Behandlungspläne zu erstellen und Medikamente zu entwickeln. Im Finanzwesen unterstützen KI-Systeme bei der Betrugsprävention, der Analyse von Finanzdaten und dem Handel an den Börsen. Im Transportwesen ermöglichen autonome Fahrzeuge und intelligente Verkehrssysteme eine effizientere und sicherere Mobilität. Im Bereich der Robotik werden KI-Technologien verwendet, um Roboter mit menschenähnlichen Fähigkeiten auszustatten, die in der Produktion, im Gesundheitswesen und in der Pflege eingesetzt werden können.

Trotz der vielfältigen Anwendungsbereiche stehen KI-Systeme vor einer Reihe von problematischen Herausforderungen. Ein zentrales Thema ist der Datenschutz. Die Verarbeitung großer Datenmengen ist für das Training von KI-Modellen unerlässlich. Dabei können jedoch personenbezogene Informationen erfasst, gespeichert und analysiert werden, was potenziell zu Datenschutzverletzungen führen kann. Die Einhaltung geltender Datenschutzgesetze und die Gewährleistung der Privatsphäre der Nutzer sind daher von entscheidender Bedeutung.

Ein weiteres Problem ist der mögliche Bias und Diskriminierung, der in KI-Systemen auftreten kann. Wenn KI-Algorithmen auf unzureichenden oder voreingenommenen Daten trainiert werden, können sie Vorurteile entwickeln und Entscheidungen treffen, die bestimmte Gruppen benachteiligen. Dies kann zu ethischen und sozialen Problemen führen und erfordert eine umfassende Prüfung und Überwachung der KI-Anwendungen.

Das Spannungsverhältnis zwischen Künstlicher Intelligenz und Datenschutzrecht ist ein aktuelles Thema, das zunehmend an Bedeutung gewinnt. Datenschutzgesetze wie die Datenschutz-Grundverordnung (DSGVO) in der Europäischen Union setzen klare Regeln für die Verarbeitung personenbezogener Daten. Unternehmen, die KI-Technologien einsetzen, müssen sicherstellen, dass sie die erforderlichen Zustimmungen einholen, die Daten sicher speichern und angemessene Maßnahmen ergreifen, um die Privatsphäre zu schützen.

Die Entwicklung der Künstlichen Intelligenz hat zweifellos beeindruckende Fortschritte gemacht und bietet viele potenzielle Vorteile in verschiedenen Anwendungsbereichen. Dennoch ist es unerlässlich, die datenschutzrechtlichen und ethischen Herausforderungen im Zusammenhang mit Künstlicher Intelligenz zu adressieren und sicherzustellen, dass die Technologie verantwortungsvoll entwickelt und eingesetzt wird, um die Privatsphäre der Nutzer zu schützen und Diskriminierung zu vermeiden.

ChatGPT hat eine mM nach durchaus passable Einleitung zum Thema KI verfasst. Vielleicht hätte es noch auf *Marvin Minsky* hinweisen können, von dem eine frühe Definition von künstlicher Intelligenz stammt. Er bezeichnete sie als *„die Wissenschaft davon, Maschinen dazu zu bringen, Dinge zu tun, deren Ausführung menschliche Intelligenz erfordert"*.[1]

Entwicklung und Umsetzung in der EU

Die EK setzte sich erst relativ spät mit dem Thema KI auseinander. So legte sie

- am 6. 5. 2015 das Papier „Strategie für einen digitalen Binnenmarkt für Europa"[2] vor, als Weiterentwicklung der „digitalen Agenda Europas".[3]
- Am 9. 3. 2018 kündigte sie in einer Pressekonferenz die Schaffung einer Expertengruppe zu KI an, die die EK bei der Bildung einer breiten *„europäischen Allianz zur künstlichen Intelligenz"* beraten sowie die Umsetzung der neuen europäischen Initiative zur künstlichen Intelligenz unterstützen sollte.
- Am 25. 4. 2018 veröffentlichte die EK eine Stellungnahme über Haftungsfragen iZm den aufstrebenden digitalen Technologien wie Internet of things, KI, fortgeschrittene Robotik und autonome Systeme.
- Am 7. 12. 2018 wurde von der EK ein koordinierter Plan für die Entwicklung und den Einsatz von künstlicher Intelligenz[4] an das europäische Parlament, den europäischen Rat, den Rat, den europäischen Wirtschafts- und Sozialausschuss sowie den Ausschuss der Regionen übermittelt.
- Am 8. 4. 2019 veröffentlichte die „Hochrangige Expertengruppe für künstliche Intelligenz", die von der EK im Juni 2018 eingesetzt wurde, Ethik-Leitlinien für eine vertrauenswürdige KI.[5] Dieses Dokument enthält ua eine Liste von Bewertungsfragen.
- Am 19. 2. 2020 veröffentlichte die EK das „Weißbuch zur künstlichen Intelligenz",[6] das politische Optionen für die Umsetzung von KI fördern und gleichzeitig die mit dieser Technologie einhergehenden Gefahren behandeln sollte.
- Am 17. 7. 2020 veröffentlichte die „Hochrangige Expertengruppe für künstliche Intelligenz" in Fortsetzung ihrer Ethik-Leitlinien vom 8. 4. 2019 eine überarbeitete Bewertungsliste in Form eines Tools zur Selbstbewertung mit der Bezeichnung ALTAI.[7]
- Am 21. 4. 2021 – also nach dreijähriger Vorbereitung – legte die EK ihren Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz vor.[8] Die KI-VO der EU gilt als fundamentaler Grundstein für die Regulierung von Künstlicher Intelligenz in der EU. Das Kernstück ist eine vierstufige Gliederung von KI-Anwendungen nach den damit verbundenen Gefahren:

[1] https://kurzelinks.de/ok92. [2] COM(2015) 192 fin, https://kurzelinks.de/hzzr. [3] KOM(2010) 245 endgültig, https://kurzelinks.de/pmai. [4] COM(2018) 795 fin, https://kurzelinks.de/y8av. [5] https://kurzelinks.de/jzx3. [6] COM (2020) 65 fin, https://kurzelinks.de/uwvc. [7] https://kurzelinks.de/vmgm. [8] COM(2021) 206 fin, https://kurzelinks.de/opgt.

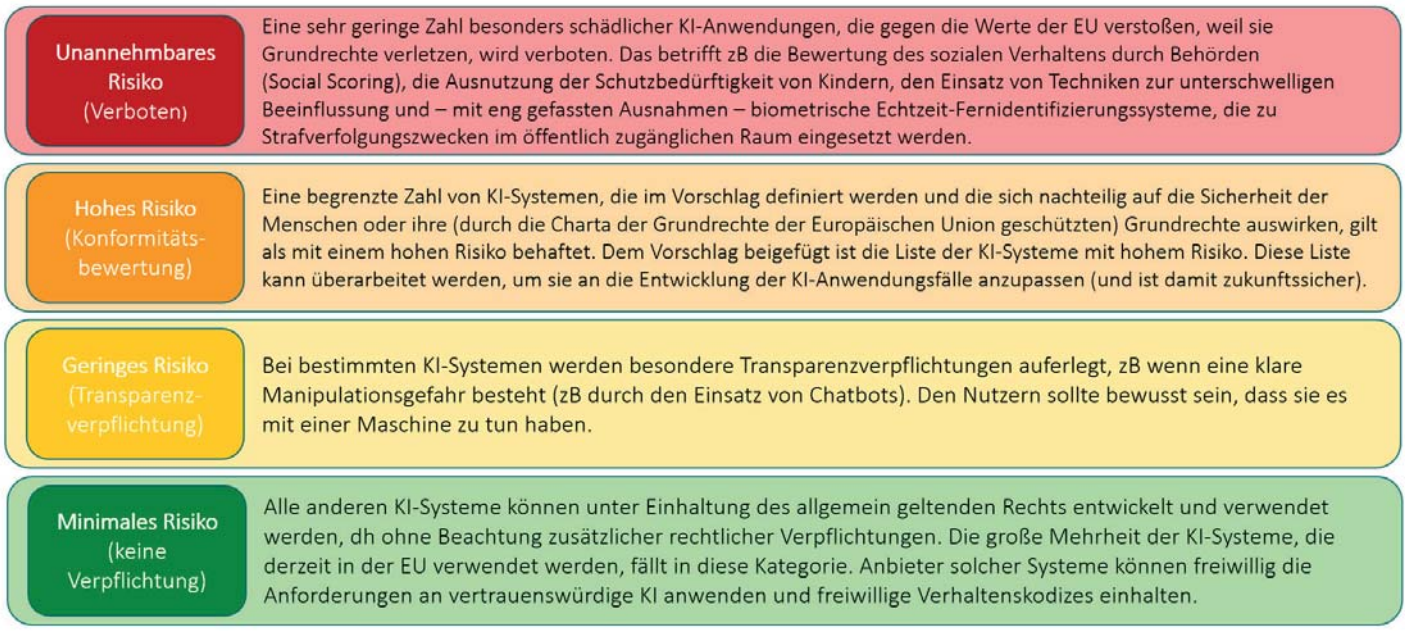

Abb 1: Vierstufige Gliederung von KI-Anwendungen

- Am 22. 12. 2021 gab der europäische Wirtschafts- und Sozialausschuss eine positive Stellungnahme zum Vorschlag der KI-VO ab, wies aber auf Verbesserungsmöglichkeiten hin.
- Am 13. 10. 2022 gab der Europäische Datenschutzbeauftragte (EDSB) seine Stellungnahme zum Vorschlag der KI-VO ab.[9]
- Am 6. 12. 2022 – also nach eineinhalbjähriger Beratung – stellte auch der Rat der europäischen Union seinen Standpunkt zur KI-VO vor.[10]
- Am 27. 4. 2023 überbrückten die Mitglieder des EP ihre Differenzen und erzielten eine vorläufige politische Einigung über die geplante KI-VO. Wesentlicher Streitpunkt war die Frage, wie mit KI-Systemen umgegangen werden soll, die keinen bestimmten Zweck verfolgen (General Purpose AI; GPAI).
- Am 11. 5. 2023 stimmten die Ausschüsse für Binnenmarkt und Verbraucherschutz (IMCO) und für bürgerliche Freiheiten, Justiz und Inneres (LIBE) über die endgültigen Kompromissänderungsanträge zur KI-VO ab und nahmen alle Änderungsanträge sowie den Gesamtbericht an. Der Kompromissvorschlag vom 9. 5. 2023 umfasst insgesamt 144 Seiten und sieht ua ein Verbot von KI für biometrische Überwachung in Echtzeit, Emotionserkennung und vorausschauende Polizeiarbeit vor.
- Am 14. 6. 2023 einigte sich das EP mit 499 zu 28 Stimmen bei 93 Enthaltungen auf eine gemeinsame Position zur KI-VO. Das Kompromisspaket umfasst 349 Seiten. Durch diese Einigung ist der Weg für den Trilog frei.[11]

Ursprünglich war geplant, die KI-VO bereits zu Beginn 2023 zu verabschieden. Ob mit einer Verabschiedung noch vor der im Juni 2024 stattfindenden Europawahl zu rechnen ist, bleibt abzuwarten.

Problematische Aspekte

Der Einsatz von KI kann dazu beitragen, die Gesundheitsversorgung zu verbessern, die Entwicklung einer neuen Generation von Produkten und Dienstleistungen zu ermöglichen, Wartungstechniken und Kundenservice zu verbessern und Energie zu sparen. KI wird auch zur Erstellung von Prognosen, für automatisierte Entscheidungsfindung, Klassifizierung und Anomalieerkennung uvm eingesetzt. Aber der Einsatz von KI bringt auch Gefahren mit sich, zB durch die Verwendung von Zahlen, die präzise erscheinen, ohne dass dies der Fall ist (sog **„Mathwashing"**), oder durch Entscheidungen bei Versicherungsanträgen, Kredit- oder Jobvergaben, die nicht selten auch von **sensiblen Daten** der Betroffenen (rassische und ethnische Zugehörigkeit, politische Meinung, religiöse oder weltanschauliche Überzeugung) beeinflusst werden.

Daher ist es beim Einsatz von KI wichtig, dass der Datenschutz besondere Beachtung findet. Hier spielt va die Frage eine wichtige Rolle, ob die KI-Anwendung den datenschutzrechtlichen Grundsätzen des Art 5 DSGVO entspricht und ob sie auf einer gültigen Rechtsgrundlage beruht sowie aus Sicht der Betroffenen transparent ist.

Die Checkliste soll Unternehmen, die in ihren automationsunterstützten Verfahren KI-Systeme direkt oder über Schnittstellen einsetzen (*„deployer"* im EP-Kompromisstext der KI-VO) – zB für Consent Management, personalisierte Werbung, Trenderkennung und -vorhersage im CRM, Beschwerdemanagement, Gesichtserkennung, automatisierte Entscheidungsfindung (ADM), Servicemanagement, Erstellung von Marketingtexten uvm –, unterstützen, ihre Anwendungen auf die Einhaltung der Bestimmungen der DSGVO zu prüfen.

Anwendungsbereich

Wie die DSGVO normiert auch die KI-VO Anforderungen an den Umgang mit Daten. Während aber bei der DSGVO der Schutz der personenbezogenen Daten im Vordergrund steht, gibt die KI-VO den Rahmen für den generellen Umgang mit Daten vor **(Daten-Governance)**. In der Begründung zum Entwurf stellt die EK klar, dass die DSGVO durch die KI-VO unberührt bleibt. Demnach gelten beide VO nebeneinander.

Da es sich bei der KI-VO noch um einen Entwurf handelt und auch noch nicht absehbar ist, wann sie tatsächlich in Kraft treten wird, wurden ihre spezifischen Bestimmungen bei der Erstellung der folgenden

[9] https://kurzelinks.de/c0dp. [10] https://kurzelinks.de/kky9. [11] https://kurzelinks.de/ag6t.

Checkliste nicht berücksichtigt. Nach Inkraftsetzung der KI-VO werden diese aber zusätzlich zu den Bestimmungen der DSGVO zu beachten sein.

Die Checkliste deckt die **Anforderungen an Entwickler** von KI-Systemen **nicht** ab. Für diese kann zB der vom Fraunhofer-Institut für Intelligente Analyse und Informationssysteme/IAIS veröffentlichte „Leitfaden zur Gestaltung vertrauenswürdiger künstlicher Intelligenz“[12] herangezogen werden. Für Medizinprodukte-Hersteller wurde vom Johner-Institut ein Leitfaden für KI bei Medizinprodukten veröffentlicht.[13]

Des Weiteren können die Leitlinien der EK für eine vertrauenswürdige KI vom 8. 4. 2019 und das Tool zur Selbstbewertung (ALTAI) vom 17. 7. 2020 genutzt werden. Auch die französische Aufsichtsbehörde CNIL stellt einen „Self-assessment guide for artificial intelligence (AI) systems“[14] auf ihrer Website zur Verfügung.

[12] https://kurzelinks.de/8ot1. [13] https://www.johner-institut.de/ai-guideline/. [14] https://kurzelinks.de/lksa.

Prüffragen

Prüffrage	ja	nein
Frage 1: Werden im Rahmen des verwendeten KI-Systems personenbezogene Daten iSd Art 4 Z 1 DSGVO verarbeitet? ***Anmerkung:*** *Falls im Rahmen des verwendeten KI-Systems keine personenbezogenen Daten verarbeitet werden, sondern nur zB Code, Bilder und Text generiert wird, und auch beim Training des Modells keine personenbezogenen Daten verwendet werden, also keine DSGVO-Relevanz besteht, ist eine weitere Auseinandersetzung mit dieser Checkliste aus datenschutzrechtlicher Sicht entbehrlich. Trifft dies jedoch zu, dann sind in beiden Fällen die datenschutzrechtlichen Bestimmungen zu beachten und möglicherweise durch verschiedene Verantwortliche wahrzunehmen. Weiters ist darauf hinzuweisen, dass die KI-VO je nach Konstellation (zB Hochrisiko-KI) eigene Maßnahmen und va eine Folgenabschätzung verlangen wird, die vom Datenschutz unabhängig ist – es reicht, wenn die KI hochriskante Auswirkungen auf Menschen hat, auch wenn die Verarbeitung nicht auf personenbezogenen Daten beruht.*		
Frage 2: Ist die Funktionsweise des verwendeten KI-Systems nachvollziehbar? ***Anmerkung:*** *Der Prozess sollte für den Verantwortlichen iSd Art 4 Z 7 DSGVO nachvollziehbar und keine „Blackbox“ sein. Der Verantwortliche ist für die Kontrolle über die Verarbeitung der Daten verantwortlich.*		
Frage 3: Ersetzt das KI-System ein anderes System? ***Anmerkung:*** *Vom Verantwortlichen ist zu analysieren, ob das geplante KI-System wirklich einen signifikanten Vorteil gegenüber dem bisher eingesetzten System bietet und va dem Grundsatz der Verhältnismäßigkeit entspricht. Der Grundsatz der Verhältnismäßigkeit bedeutet, dass der Verantwortliche ein ausgewogenes Verhältnis zwischen den eingesetzten Mitteln und dem geplanten Ziel beachten muss. Va darf ein signifikanter Vorteil des KI-Einsatzes nicht zu einem erhöhten Risiko für die Betroffenen führen.*		
Frage 4: Kann der Einsatz des KI-Systems direkt oder indirekt negative Auswirkungen auf besonders schutzwürdige Personen wie Kinder, Patienten oder Mitarbeiter haben? ***Anmerkung:*** *Beim Einsatz der KI für den oa schutzwürdigen Personenkreis sind bei Kindern die Bestimmungen des Art 8 DSGVO, bei Patienten jene des Art 9 DSGVO und bei Dienstnehmern das Ungleichgewicht mit der Arbeitgeberseite zu berücksichtigen.*		
Frage 5: Werden durch das KI-System besondere Kategorien personenbezogener Daten verarbeitet (sog sensible Daten)? ***Anmerkung:*** *Sensible Daten dürfen nur dann verarbeitet werden, wenn ein Ausnahmetatbestand des Art 9 Abs 2 DSGVO vorliegt.*		
Frage 6: Ist die datenschutzrechtliche Rollenverteilung eindeutig festgelegt? ***Anmerkung:*** *In der Regel wird der Verantwortliche iSd Art 4 Z 7 DSGVO für die Verwendung des eingesetzten KI-Systems verantwortlich sein und der KI-Systemanbieter die Rolle des Auftragsverarbeiters iSd Art 4 Z 8 DSGVO einnehmen. Falls der KI-Systemanbieter ausschließlich diese weisungsgebundene Rolle einnimmt, ist nach den Bestimmungen des Art 28 DSGVO ein Auftragsverarbeitungsvertrag abzuschließen. Verwendet jedoch der KI-Systemanbieter die ihm vom Verantwortlichen übermittelten Daten auch für eigene Zwecke wie zB zum Training des KI-Systems, liegt eine gemeinsame Verantwortlichkeit iSd Art 26 DSGVO vor; sa Anm zu Frage 1.*		
Frage 7: Findet durch das KI-System eine automatisierte Entscheidungsfindung statt? ***Anmerkung:*** *Sog ADM-Systeme (Algorithmic Decision Making) werden in vielen Bereichen – zB Überprüfung der Kreditwürdigkeit, Recruiting, Versicherungsvertragsabschlüsse – eingesetzt. IdZ sind die Bestimmungen des Art 22 DSGVO zu beachten und die betroffenen Personen über die automatische Entscheidungsfindung im Rahmen der Informationspflichten der Art 13 und 14 DSGVO entsprechend zu informieren. Bei Einsatz solcher Systeme ist fast sicher eine Datenschutz-Folgenabschätzung (DSFA) gem Art 35 DSGVO – noch vor Einsatz des ADM-Systems – erforderlich; s Anm zu Frage 14.*		
Frage 8: Wird ChatGPT in der Datenanwendung verwendet? ***Anmerkung:*** *Bei Nutzung von ChatGPT sollte versucht werden, der Nutzung der vom Verantwortlichen übermittelten Daten zu eigenen Zwecken der OpenAI zu widersprechen. Dies sollte auch bei anderen Anbietern versucht werden.*		
Frage 9: Werden beim Einsatz von Chatbots die Nutzer darüber informiert, dass sie mit einem Bot anstatt mit einem Menschen sprechen? ***Anmerkung:*** *ISd in Art 5 Abs 1 lit a DSGVO geforderten Transparenzgebotes sind die Nutzer über den Einsatz von Chatbots zu informieren.*		
Frage 10: Auf welcher Rechtsgrundlage erfolgt die Nutzung des verwendeten KI-Systems? ***Anmerkung:*** *Häufig wird die Nutzung des KI-Systems auf Basis der berechtigten Interessen des Verantwortlichen gem Art 6 Abs 1 lit f DSGVO erfolgen, wobei die Schutzinteressen der betroffenen Person nicht überwiegen dürfen. Auch die Rechtsgrundlage des Art 6 Abs 1 lit b (Vertragserfüllung) kann herangezogen werden, zB wenn das KI-System Service- und Assistenzfunktionen zur Beantwortung von Kundenanfragen bereitstellt. Als weitere mögliche Rechtsgrundlage kommt auch die Einwilligung des Art 6 Abs 1 lit a in Betracht, die allerdings den Nachteil des jederzeitigen Widerrufs durch die betroffene Person in sich birgt.*		
Frage 11: Wurde vor Einsatz eines KI-Algorithmus geprüft, ob ein grundrechtskonformer Einsatz überhaupt möglich ist? ***Anmerkung:*** *Falls die Überprüfung Zweifel zB an der ausreichenden Nachvollziehbarkeit, Überprüfbarkeit und Beherrschbarkeit ergibt, sollte auf den Einsatz dieses Algorithmus verzichtet werden.*		
Frage 12: Liegen transparente und nachvollziehbare Informationen über den Algorithmus vor? ***Anmerkung:*** *Informationen über den Algorithmus sollten aussagekräftig, umfassend und verständlich sein. Sie sollten neben einer Beschreibung der Ein- und Ausgabedaten va die im Algorithmus enthaltene Logik und ihre Auswirkungen beschreiben.*		
Frage 13: Sind die Sicherheit und Vertrauenswürdigkeit des Algorithmus sichergestellt sowie eine menschliche Kontrolle im Bedarfsfall vorgesehen? ***Anmerkung:*** *Vertrauenswürdigkeit und Sicherheit sowie va der Schutz vor Manipulationen des verwendeten Algorithmus sind durch geeignete technische und organisatorische Maßnahmen sicherzustellen. Zur Gewährleistung der Überprüfbarkeit sollte der Source-Code des eingesetzten Algorithmus beim Verantwortlichen der Verarbeitung vorliegen. Des Weiteren ist laufendes Monitoring notwendig.*		

Prüffrage	ja	nein
Frage 14: Wurde in Bezug auf die Nutzung des KI-Systems eine DSFA durchgeführt? ***Anmerkung:*** *Art 35 DSGVO fordert insb bei Verwendung neuer Technologien, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, die Durchführung einer DSFA. § 2 Abs 2 Z 4 DSFA-V sieht ebenfalls die Durchführung einer DSFA beim Einsatz von KI-Systemen vor.*		
Frage 15: Wird in der Art 13 und 14 DSGVO-Information auf die Verwendung des KI-Systems hingewiesen? ***Anmerkung:*** *In Erfüllung des Grundsatzes der fairen und transparenten Verarbeitung personenbezogener Daten ist der Betroffene im Rahmen der Informationspflichten des Art 13 und 14 DSGVO entsprechend zu informieren. Besonderer Wert ist bei dieser Information auf den Grundsatz der Transparenz und die Erkennbarkeit des KI-Systems zu legen; der Prozess sollte für den Betroffenen nachvollziehbar sein. Die involvierte Logik sowie die Tragweite der Verarbeitung müssen transparent erklärt werden.*		
Frage 16: Wird der Grundsatz der Datenminimierung des Art 5 Abs 1 lit c DSGVO beachtet? ***Anmerkung:*** *Aufgrund der Bestimmungen des Art 5 Abs 1 lit c DSGVO dürfen nur Daten erhoben werden, die zur Erfüllung des erhobenen Zweckes erforderlich sind, dh die Daten müssen relevant und auf das Notwendigste beschränkt sein. IdZ ist auch auf das von der EU geförderte Projekt Feature Cloud[15] zu verweisen, das auf der Idee eines föderativen dezentralen maschinellen Lernens (federated machine learning) basiert und mit in die Software-Architektur integrierten Datenschutz nutzt. Zentrale Eigenschaften der Methode bestehen darin, dass keine vertraulichen Daten über irgendwelche Kommunikationskanäle übermittelt werden und dass die Daten nicht in nur einer zentralen Stelle gespeichert werden. Dh, sensible Datensätze bleiben lokal gespeichert (zB medizinische Daten in den Spitälern oder bei Forschungsinstituten) und nur aggregierte sensible personenbezogene Daten werden ausgetauscht. Je mehr federated machine learning entwickelt ist, desto mehr ist es als Alternative nach dem „Stand der Technik" zu sehen.*		
Frage 17: Wurde der Einsatz des KI-Systems im Verzeichnis der Verarbeitungstätigkeiten erfasst? ***Anmerkung:*** *Im gem Art 30 DSGVO zu führenden Verzeichnis von Verarbeitungstätigkeiten ist auch das eingesetzte KI-System anzuführen.*		
Frage 18: Werden durch das eingesetzte KI-System personenbezogene Daten in ein Drittland ohne angemessenes Datenschutzniveau übermittelt? ***Anmerkung:*** *Befindet sich der KI-Systemanbieter in einem Drittland ohne angemessenes Datenschutzniveau, sind die Bestimmungen zum internationalen Datenverkehr gem Art 44ff DSGVO zu beachten.*		
Frage 19: Wird beim Einsatz des verwendeten KI-Systems der Grundsatz des Art 25 DSGVO „Privacy by Design and by Default" beachtet? ***Anmerkung:*** *Als entsprechende Maßnahmen iZm den Bestimmungen des Art 25 DSGVO sind va Pseudonymisierung, Datenminimierung sowie Verschlüsselung zu nennen. Aber auch die Einrichtung eines strengen Berechtigungskonzepts nach dem „Need-to-know"-Prinzip, die automatische Löschung von personenbezogenen Daten nach vorgegebenem Zeitablauf oder die Kennzeichnung von Pflichtfeldern in Web-Formularen tragen zur Erfüllung des Art 25 bei; sa Anm zum federated machine learning bei Frage 16.*		
Frage 20: Können die Rechte der Betroffenen gem Art 15 bis 21 DSGVO erfüllt werden? ***Anmerkung:*** *Im Zuge der datenschutzrechtlichen Verantwortlichkeit ist besonders die Verpflichtung zur Erfüllung der Rechte der betroffenen Person zu beachten und entsprechende Prozesse auszuarbeiten.*		

Dako 2023/44

[15] https://featurecloud.eu.

Zum Thema

Über den Autor

Prof. KommR Hans-Jürgen Pollirer ist Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH und fachkundiger Laienrichter für Datenschutz am BVwG sowie juristischer und technischer EuroPriSe-Gutachter. E-Mail: hj.pollirer@secur-data.at

Danksagung

Für wertvolle Empfehlungen und Hinweise bei der Erstellung der Checkliste bedankt sich der Autor beim wissenschaftlichen Leiter und Gesellschafter des Research Institute – Digital Human Rights Center, Herrn Ing. Dr. Christof Tschohl.

Literatur

- *Specht*, Die 50 wichtigsten Themen der Digitalisierung (2018)
- *Burgstaller/Hermann/Lampesberger*, Künstliche Intelligenz (2019)
- *Bünte*, Die chinesische KI-Revolution (2020)
- *Lämmel/Cleve*, Künstliche Intelligenz[5] (2020)
- *Paaß/Hecker*, Künstliche Intelligenz (2020)
- *Brandolisio/Leitl/Golta*, The AI Toolbook (2021)
- *Ertel*, Grundkurs Künstliche Intelligenz[5] (2021)
- *Misselhorn*, Künstliche Intelligenz und Empathie (2021)
- *Precht*, Künstliche Intelligenz und der Sinn des Lebens (2021)