Künstliche Intelligenz versus Sozialdatenschutz

Mathias Schadly
AOK Bayern – Die Gesundheitskasse

Gesundheit nehmen wir persönlich.
AOK Bayern. Die Gesundheitskasse.

Bereich Datenschutz
25.10.2023

Überblick

- Ausgangslage
- Herangehensweise
- Datenschutzrechtliche Verantwortung
- Ausschlusskriterien
- Bewertung der Kritikalität
- Datenschutzrechtliche Aspekte vor dem Trainieren mit (Krankenkassen-/Gesundheitsdaten) Daten
- Fazit
- Backup: Verfügbares Quellenmaterial

Ausgangslage

- Sozialversicherungen als K.d.ö.R. und „Treuhändische Verwaltung des Versichertenvermögens“
- Qualifizierung ist auf SV-Fachlichkeit ausgerichtet
- Digitalisierung fordert kontinuierliche Anstrengungen und Wandel in den Verwaltungen
- stetig wachsende Regulatorik inkl. Datenschutzrecht
- Kundenzentrierung fordert zu Recht erste Priorität der Ressourcen… usw.

→ und jetzt noch KI verstehen, einführen und Compliance sicherstellen?

Meine Realität

Sozialgesetzbuch (SGB) Viertes Buch (IV) - Gemeinsame Vorschriften für die Sozialversicherung - (Artikel I des Gesetzes vom 23. Dezember 1976, BGBl. I S. 3845)
§ 30 Eigene und übertragene Aufgaben

(1) Die Versicherungsträger dürfen nur Geschäfte zur Erfüllung ihrer gesetzlich vorgeschriebenen oder zugelassenen Aufgaben führen und ihre Mittel nur für diese Aufgaben sowie die Verwaltungskosten verwenden.
(2) Den Versicherungsträgern dürfen Aufgaben anderer Versicherungsträger und Träger öffentlicher Verwaltung nur auf Grund eines Gesetzes übertragen werden; dadurch entstehende Kosten sind ihnen zu erstatten. Verwaltungsvereinbarungen der Versicherungsträger zur Durchführung ihrer Aufgaben bleiben unberührt.
(3) Versicherungsträger können die für sie zuständigen obersten Bundes- und Landesbehörden insbesondere in Fragen der Rechtsetzung kurzzeitig personell unterstützen. Dadurch entstehende Kosten sind ihnen grundsätzlich zu erstatten; Ausnahmen werden in den jeweiligen Gesetzen zur Feststellung der Haushalte von Bund und Ländern festgelegt.

Bayerisches Staatsministerium für Gesundheit und Pflege

Bayerisches Landesprüfungsamt für Sozialversicherung

DSK
DATENSCHUTZKONFERENZ

Sozialgesetzbuch (SGB) Viertes Buch (IV) - Gemeinsame Vorschriften für die Sozialversicherung - (Artikel I des Gesetzes vom 23. Dezember 1976, BGBl. I S. 3845)
§ 69 Ausgleich, Wirtschaftlichkeit und Sparsamkeit, Kosten- und Leistungsrechnung, Personalbedarfsermittlung

(1) Der Haushalt ist in Einnahme und Ausgabe auszugleichen.
(2) Bei der Aufstellung und Ausführung des Haushaltsplans hat der Versicherungsträger sicherzustellen, dass er die ihm obliegenden Aufgaben unter Berücksichtigung der Grundsätze der Wirtschaftlichkeit und Sparsamkeit erfüllen kann.
(3) Für alle finanzwirksamen Maßnahmen sind angemessene Wirtschaftlichkeitsuntersuchungen durchzuführen.
(4) In geeigneten Bereichen ist eine Kosten- und Leistungsrechnung einzuführen.
(5) Die Träger der Kranken- und Rentenversicherung, die gewerblichen Berufsgenossenschaften, die Unfallversicherungsträger der öffentlichen Hand sowie die Sozialversicherung für Landwirtschaft, Forsten und Gartenbau führen in geeigneten Bereichen ein Benchmarking durch.
(6) Die Sozialversicherungsträger dürfen Planstellen und Stellen nur ausbringen, soweit sie unter Anwendung angemessener und anerkannter Methoden der Personalbedarfsermittlung begründet sind. Die Erforderlichkeit der im Haushaltsplan ausgebrachten Planstellen und Stellen ist bei gegebenem Anlass, im Übrigen regelmäßig zu überprüfen.

Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung - (Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477)
§ 284 Sozialdaten bei den Krankenkassen

(1) Die Krankenkassen dürfen Sozialdaten für Zwecke der Krankenversicherung nur erheben und speichern, soweit diese für
1. die Feststellung des Versicherungsverhältnisses und der Mitgliedschaft, einschließlich der für die Anbahnung eines Versicherungsverhältnisses erforderlichen Daten,
2. die Ausstellung des Berechtigungsscheines und der elektronischen Gesundheitskarte,
3. die Feststellung der Beitragspflicht und der Beiträge, deren Tragung und Zahlung,
4. die Prüfung der Leistungspflicht und der Erbringung von Leistungen an Versicherte einschließlich der Voraussetzungen von Leistungsbeschränkungen, die Bestimmung des Zuzahlungsstatus und die Durchführung der Verfahren bei Kostenerstattung, Beitragsrückzahlung und der Ermittlung der Belastungsgrenze,
5. die Unterstützung der Versicherten bei Behandlungsfehlern,
6. die Übernahme der Behandlungskosten in den Fällen des § 264,
7. die Beteiligung des Medizinischen Dienstes oder das Gutachterverfahren nach § 87 Absatz 1c,
8. die Abrechnung mit den Leistungserbringern, einschließlich der Prüfung der Rechtmäßigkeit und Plausibilität der Abrechnung,
9. die Überwachung der Wirtschaftlichkeit der Leistungserbringung,
10. die Abrechnung mit anderen Leistungsträgern,
11. die Durchführung von Erstattungs- und Ersatzansprüchen,
12. die Vorbereitung, Vereinbarung und Durchführung von von ihnen zu schließenden Vergütungsverträgen,
13. die Vorbereitung und Durchführung von Modellvorhaben, die Durchführung des Versorgungsmanagements nach § 11 Abs. 4, die Durchführung von Verträgen zur hausarztzentrierten Versorgung, zu besonderen Versorgungsformen und zur ambulanten Erbringung hochspezialisierter Leistungen, einschließlich der Durchführung von Wirtschaftlichkeitsprüfungen und Qualitätsprüfungen,
14. die Durchführung des Risikostrukturausgleichs nach den §§ 266 und 267 sowie zur Gewinnung von Versicherten für die Programme nach § 137g und zur Vorbereitung und Durchführung dieser Programme,
15. die Durchführung des Entlassmanagements nach § 39 Absatz 1a,
16. die Auswahl von Versicherten für Maßnahmen nach § 44 Absatz 4 Satz 1 und nach § 39b sowie zu deren Durchführung,
17. die Überwachung der Einhaltung der vertraglichen und gesetzlichen Pflichten der Leistungserbringer von Hilfsmitteln nach § 127 Absatz 7,
18. die Erfüllung der Aufgaben der Krankenkassen als Rehabilitationsträger nach dem Neunten Buch,
19. die Vorbereitung von Versorgungsinnovationen, die Information der Versicherten und die Unterbreitung von Angeboten nach § 68b Absatz 1 und 2 sowie
20. die administrative Zurverfügungstellung der elektronischen Patientenakte sowie für das Angebot zusätzlicher Anwendungen im Sinne des § 345 Absatz 1 Satz 1

erforderlich sind. Versichertenbezogene Angaben über ärztliche Leistungen dürfen auch auf maschinell verwertbaren Datenträgern gespeichert werden, soweit dies für die in Satz 1 Nr. 4, 8, 9, 10, 11, 12, 13, 14 und § 305 Absatz 1 bezeichneten Zwecke erforderlich ist. Versichertenbezogene Angaben über ärztlich verordnete Leistungen dürfen auf maschinell verwertbaren Datenträgern gespeichert werden, soweit dies für die in Satz 1 Nr. 4, 8, 9, 10, 11, 12, 13, 14 und § 305 Abs. 1 bezeichneten Zwecke erforderlich ist. Im Übrigen gelten für die Datenerhebung und -speicherung die Vorschriften des Ersten und Zehnten Buches.
(2) Im Rahmen der Überwachung der Wirtschaftlichkeit der vertragsärztlichen Versorgung dürfen versichertenbezogene Leistungs- und Gesundheitsdaten auf maschinell verwertbaren Datenträgern nur gespeichert werden, soweit dies für Stichprobenprüfungen nach § 106a Absatz 1 Satz 1 oder § 106b Absatz 1 Satz 1 erforderlich ist.
(3) Die rechtmäßig erhobenen und gespeicherten versichertenbezogenen Daten dürfen nur für die Zwecke der Aufgaben nach Absatz 1 in dem jeweils erforderlichen Umfang verarbeitet werden, für andere Zwecke, soweit dies durch Rechtsvorschriften des Sozialgesetzbuchs angeordnet oder erlaubt ist. Die Daten, die nach § 295 Abs. 1b Satz 1 an die Krankenkasse übermittelt werden, dürfen nur zu Zwecken nach Absatz 1 Satz 1 Nr. 4, 8, 9, 10, 11, 12, 13, 14, 19 und § 305 Abs. 1 versichertenbezogen verarbeitet werden und nur, soweit dies für diese Zwecke erforderlich ist; für die Verarbeitung dieser Daten zu anderen Zwecken ist der Versichertenbezug vorher zu löschen.
(4) Zur Gewinnung von Mitgliedern dürfen die Krankenkassen Daten verarbeiten, wenn die Daten allgemein zugänglich sind, es sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Ein Abgleich der erhobenen Daten mit den Angaben nach § 291a Absatz 2 Nummer 2 bis 5 ist zulässig. Im Übrigen gelten für die Datenverarbeitung die Vorschriften des Ersten und Zehnten Buches.

Die Prüfdienste des Bundes
und der Länder informieren

Leitfaden

Elektronische Kommunikation
und
Digitalisierung in der Sozialversicherung

GKV Spitzenverband

Zehntes Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - (SGB X)
§ 67c Zweckbindung sowie Speicherung, Veränderung und Nutzung von Sozialdaten zu anderen Zwecken

(1) Die Speicherung, Veränderung oder Nutzung von Sozialdaten durch die in § 35 des Ersten Buches genannten Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden gesetzlichen Aufgaben nach diesem Gesetzbuch erforderlich ist und für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.
(2) Die nach Absatz 1 gespeicherten Daten dürfen von demselben Verantwortlichen für andere Zwecke nur gespeichert, verändert oder genutzt werden, wenn
1. die Daten für die Erfüllung von Aufgaben nach anderen Rechtsvorschriften dieses Gesetzbuches als diejenigen, für die sie erhoben wurden, erforderlich sind,
2. es zur Durchführung eines bestimmten Vorhabens der wissenschaftlichen Forschung oder Planung im Sozialleistungsbereich erforderlich ist und die Voraussetzungen des § 75 Absatz 1, 2 oder 4a Satz 1 vorliegen.

(3) Eine Speicherung, Veränderung oder Nutzung von Sozialdaten ist zulässig, wenn sie für die Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für den Verantwortlichen oder für die Wahrung oder Wiederherstellung der Sicherheit und Funktionsfähigkeit eines informationstechnischen Systems durch das Bundesamt für Sicherheit in der Informationstechnik erforderlich ist. Das gilt auch für die Veränderung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit nicht überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen.
(4) Sozialdaten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verändert, genutzt und in der Verarbeitung eingeschränkt werden.
(5) Für Zwecke der wissenschaftlichen Forschung oder Planung im Sozialleistungsbereich erhobene oder gespeicherte Sozialdaten dürfen von den in § 35 des Ersten Buches genannten Stellen nur für ein bestimmtes Vorhaben der wissenschaftlichen Forschung im Sozialleistungsbereich oder der Planung im Sozialleistungsbereich verändert oder genutzt werden. Die Sozialdaten sind zu anonymisieren, sobald dies nach dem Forschungs- oder Planungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Planungszweck dies erfordert.

AOK

Herangehensweise

- Systematisierung des Themenkomplexes und Erstellung einer internen Arbeitshilfe + angepasstes Template für Datenschutzfolgenabschätzung (Klärung Definitionen etc.)
- 5-Stufen-Modell BSI
  - Stufe 0 – Mensch entscheidet
  - Stufe 1 – Assistiertes Entscheiden (Bsp. Tabellenkalkulation)
  - Stufe 2 – Teilweises Entscheiden (Bsp. Intelligente E-Mail-Klassifikation oder RPA in Sachbearbeitung)
  - Stufe 3 – Geprüftes Entscheiden (Bsp. Krankenhausrechnungsprüfung)
  - Stufe 4 – Delegiertes Entscheiden
  - Stufe 5 – Autonomes Entscheiden

Datenschutzrechtliche Verantwortung (Article 3 AI Act to come)

- Rolle als „Anbieter“ oder „Nutzer“- Controller/Processor/Joint Controllership nach DSGVO?
- Aufgabenzuweisung im SGB nach § 30 SGB IV klären (finden?)
- besondere DSGVO/SGB-Herausforderungen
  - Transparenzpflichten und Betroffenenrechte
  - Nachweis Datenschutzfreundliche Technik und Voreinstellungen
  - Auftragsverarbeitung in der Cloud und Drittstaaten (§80 Abs. 2 SGB X)
  - Dokumentation der Risiken durch den Einsatz von Methoden des maschinellen Lernens (neue Technologie, Art. 35 DSGVO), ggf. Konsultationspflichten bei der Aufsichtsbehörde

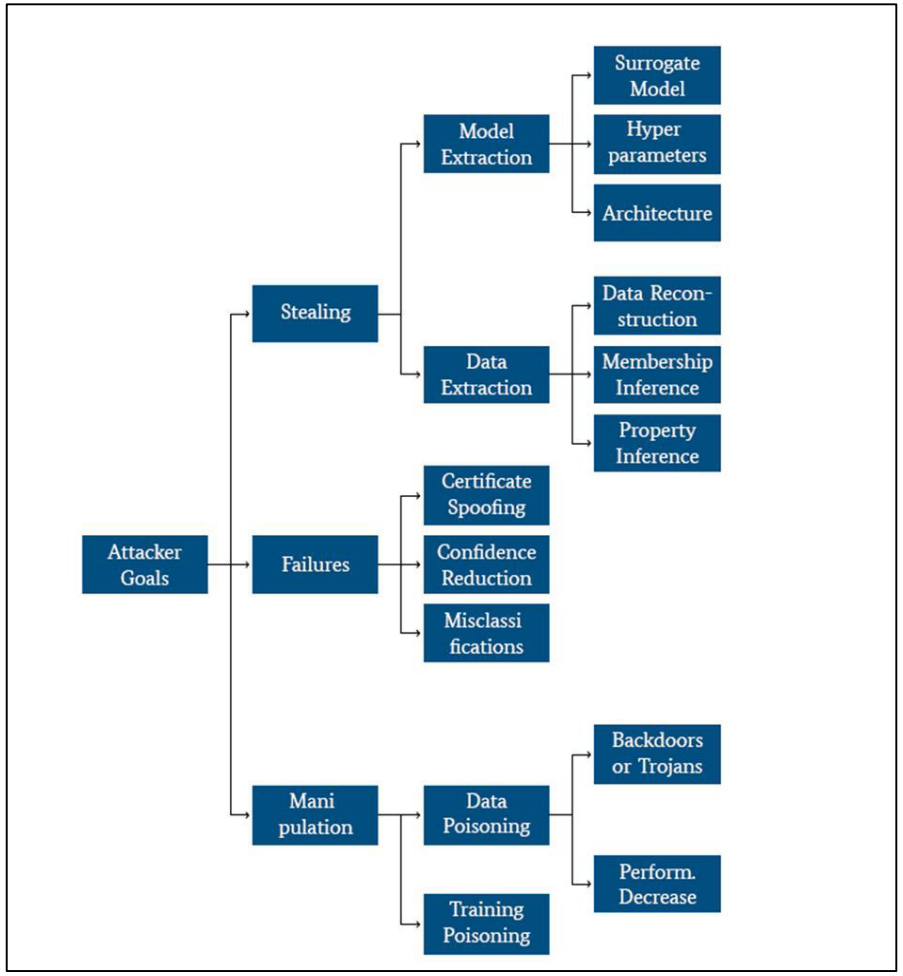
Ausschlusskriterien I
(Article 5 AI Act to come)

- Rolle als „Anbieter“ oder „Nutzer“- Controller/Processor/Joint Controllership nach DSGVO?
- Aufgabenzuweisung im SGB nach § 30 SGB IV klären (finden?)
- besondere DSGVO/SGB-Herausforderungen
  - Transparenzpflichten und Betroffenenrechte
  - Nachweis Datenschutzfreundliche Technik und Voreinstellungen
  - Auftragsverarbeitung in der Cloud und Drittstaaten (§80 Abs. 2 SGB X)
  - Dokumentation der Risiken durch den Einsatz von Methoden des maschinellen Lernens (neue Technologie, Art. 35 DSGVO), ggf. Konsultationspflichten bei der Aufsichtsbehörde

Ausschlusskriterien II (Article 5 AI Act to come)

Bestimmung der Durchführbarkeit der Datenverarbeitung (Ausschlusskriterien)
Ist die DS-rechtliche Verantwortlichkeit für den Einsatz der künstlichen Intelligenz ungeklärt ?
Wird bei der Automation der Entscheidungsfindung die Stufe 5 erreicht?
Wenn automatisierte Entscheidungen getroffenen werden, wird der Prozess derart ausgestaltet, dass negative Entscheidungen (z.B. Verwehrung einer Verwaltungsleistung) ohne Prüfung durch einen Mitarbeiter getroffen werden?
Fehlt eine Rechtsgrundlage zum Einsatz der KI?
Besitzt die künstliche Intelligenz die Fähigkeit zum kontinuierlichen/ selbstständigen Lernen?
Gibt es eine unterschwellige Beeinflussung außerhalb des Bewusstseins einer Person, um das Verhalten einer Person zu beeinflussen?
Werden Schwächen oder Schutzbedürftigkeiten einer bestimmten Gruppe von Personen aufgrund personenbezogener Merkmale ausgenutzt, um das Verhalten einer dieser Gruppen angehörigen Personen wesentlich zu beeinflussen?
Gibt es eine Bewertung/ Klassifizierung der Vertrauenswürdigkeit natürlicher Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens bekannter oder vorhergesagter personlicher Eigenschaften oder Persönlichkeitsmerkmale, wobei die soziale Bewertung zu einer Benachteiligung führt oder führen könnte?

Bewertung der Kritikalität (Article 6 AI Act to come)



Hochgradige Risiken	Evasion-Angriffe	Poisoning-Angriffe	Extraction-Angriffe
Öffentlich verfügbarer KI-Dienst	D	I	D
Unbekannte Herkunft der Trainingsdaten	I	D	I
Unbekannte Herkunft der Inferenzdaten	D	I	D
Autonome Entscheidungen durch die KI	D	I	D
Vollständige Ausgaben des Modells	D	I	D
Ungeregelter Zugriff auf das KI-Modell	D	D	D
Öffentlich verfügbares Modell	D	D	D
Kontinuierliches Lernen	I	D	I

Mögliche risikominimierende Maßnahmen nach Angriffstypen

Datenschutzrechtliche Aspekte vor dem Trainieren mit (Krankenkassen-/Gesundheitsdaten) Daten

- Klassifikation von Daten und Informationen ist unerlässlich
  - anonyme + statistische Informationen
  - pbD
  - besondere pbD
  - Sozialdaten
  - Betriebs- und Geschäftsgeheimnisse
  - Gleichstellung von pseudonymisierten Daten mit pbD bedenken (EG 26 DSGVO)
- Legitime Zweckänderung ausgehend vom Zweckbindungsgrundsatz nach DSGVO und SGB begründen
- Datenminimierungsgrundsatz der DSGVO einhalten
- Schutz von Rechten nach dem Training

Fazit I

- Nicht mal einfach so machbar
- Know How entsprechend der übernommenen Verantwortung ist erforderlich und aufzubauen. Dafür braucht es Qualifizierungs-Angebote.
- Schon die bestehende (datenschutz-) Regulatorik ist anspruchsvoll und wird durch den AI Act in der Komplexität weiter erhöht.
- Bevor die KI den Arbeitsalltag erleichtert bedeutet die Implementierung einen enormen Invest und Change (vom Selbermachen zum Überwachen)

Fazit II

- **AI Act Pro**
  - Definierte Rechtsbegriffe und gemeinsame Sprache in EU
  - Rückgriff auf Zertifikate durch Verantwortliche (irgendwann) möglich
- **AI Act Contra**
  - Mehr staatliche Regulatorik und Überwachung (Innovationshemmnis?)
  - Redundanzen und begriffliche Abweichungen vom DSGVO-Recht
  - Rechtssetzung läuft Realität und Markterfordernissen bereits jetzt hinterher

Ich freue mich auf die Fragen aus dem Chat.

Verfügbares Quellenmaterial

- **Was hat uns bisher geholfen?**
  - Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, zuletzt abgerufen am 03.11.2022 unter: https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf
  - Bitkom: Leitfaden Künstliche Intelligenz verstehen als Automation des Entscheidens, abgerufen am 22. September 2022 von https://www.bitkom.org/Bitkom/Publikationen/Kuenstliche-Intelligenz-verstehen-als-Automation-des-Entscheidens.html
  - SAE International (2021). Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles SAE International Standard J3016. Abgerufen am 20. September 2022 von https://www.sae.org/standards/content/j3016_201806/
  - Künstliche Intelligenz in der Medizin, zuletzt aufgerufen am 26.09.2022: https://www.datarevenue.com/de-blog/kuenstliche-intelligenz-in-der-medizin
  - BSI, Security of AI-Systems

Anschrift: AOK Bayern – Die Gesundheitskasse
Zentrale
Bereich Datenschutz
Mathias Schadly
Carl-Wery-Straße 28
81739 München

Telefon: 089 62730-353

Mobil: 01520 1561930

E-Mail: mathias.schadly@by.aok.de