ChatGPT, Bard & Co.

Wie künstliche Intelligenz die Gesundheitswirtschaft verändert und welche Rolle der Datenschutz dabei spielt

Die Digitalisierung in der Gesundheitswirtschaft schreitet auch mit speziellem Blick auf die Künstliche Intelligenz (KI) unaufhaltsam und rasant voran. Der Einsatz von KI in der Radiologie oder die Verwendung von ChatGPT bilden dabei nur den Anfang. Welche Auswirkungen diese Entwicklungen auf den Datenschutz haben, beschreiben David Grosse-Dütting, Manager Curacon GmbH Wirtschaftsprüfungsgesellschaft, & Dr. Uwe Günther, Partner Curacon GmbH Wirtschaftsprüfungsgesellschaft und Geschäftsführer Sanovis GmbH, in diesem Beitrag.

Spätestens die Veröffentlichung von ChatGPT im November 2022 hat einen Hype in Bezug auf Nutzung Künstlicher Intelligenz (KI) ausgelöst und das Thema der breiten Öffentlichkeit bekannt gemacht. Mancher Experte ist der Meinung, dass die KI viele Wirtschaftszweige grundlegend verändern oder sogar ganz obsolet machen könnte. Und tatsächlich hat der Dienst innerhalb weniger Monate eine enorme Verbreitung gefunden. So ergab eine Umfrage in den USA, dass bereits 43 % aller Berufstätigen KI-Tools für ihre Arbeit nutzen.[1] Und Bill Gates bezeichnete in seinem Blog ChatGPT als revolutionärste Entwicklung der vergangenen 40 Jahre[2].

Bedenken nehmen zu

Gleichzeitig mehren sich auch die kritischen Stimmen zur KI. Im März forderte eine Gruppe von 1.000 Experten aus der Tech-Branche und Forschung in einem offenen Brief[3] ein Moratorium für die Entwicklung Künstlicher Intelligenz. „KI-Systeme mit einer Intelligenz, die Menschen Konkurrenz macht, können große Risiken für Gesellschaft und Menschheit bergen", heißt es dort. Daher sollten zunächst gemeinsame Sicherheitsstandards für die Entwicklung und den Einsatz von KI festgelegt werden. Vor allem Branchen, die sicherheitskritisch sind oder große Bedeutung für den Einzelnen haben, können die Risiken besonders leistungsfähiger KI-Systeme erheblich sein.

Bereits im Jahr 2021 gelang es dem Team um den Datenforscher Nicholas Carlini durch eine data extraction and reconstruction attack, Teile der Trainingsdaten des Sprachmodells GPT-2 zu rekonstruieren – darunter auch persönliche Daten wie Namen, Telefonnummern und E-Mail-Adressen.[4] Die Forscher kommen zu dem Schluss, dass data extraction attacks nicht nur im akademischen Kontext durchführbar sind, sondern sehr wohl eine große praktische Relevanz haben und ihre Bedeutung in Zukunft zunehmen wird.

Dr. Uwe Günther, Partner Curacon GmbH Wirtschaftsprüfungsgesellschaft und Geschäftsführer Sanovis GmbH.
Partner Curacon GmbH Wirtschaftsprüfungsgesellschaft und Geschäftsführer Sanovis GmbH. Als Leiter der Geschäftsfelder IT-Management und Datenschutz liegen die Fachgebiete von Dr. Uwe Günther sowohl in der IT als auch im betriebswirtschaftlichen Bereich. Dabei gilt er als ausgewiesener Experte für die Beratungsschwerpunkte IT-Strategie, IT-Management, Datenschutz und IT-Sicherheit.

Es seien daher Maßnahmen zu ergreifen, um bereits beim Training der KI-Modelle mögliche negative Auswirkungen auf die Privatsphäre zu vermeiden

Neue Anwendungsmöglichkeiten in der Gesundheitswirtschaft

Die möglichen Anwendungsfälle und Nutzungsmöglichkeiten sind auch in der Gesundheitswirtschaft scheinbar unbegrenzt Sie reichen von der Patientenkommunikation im Vorfeld einer Behandlung, über die Befundung von EKGs, radiologischen Befunden und Laborparametern, der automatischen Erstellung von Arztbriefen und Dienstplänen bis hin zur Ableitung von Therapieempfehlungen oder Robotern, die Unterstützung in Pflege und Betreuung leisten sollen Naturgemäß sind die Risiken aufgrund der hohen Sensitivität der Daten im Gesundheitswesen besonders groß

Da die KI-Modelle abhängig von den Trainingsdaten sind, können die Ergebnisse der Modelle diskriminierend wirken, wenn in den Trainingsdaten Menschen mit bestimmten Merkmalen unterrepräsentiert sind So zeigte die Netflix-Dokumentation „Coded Bias“[5] aus dem Jahr 2020, dass die Aussagekraft von Algorithmen und Gesichtserkennungssoftwares bei Menschen mit dunkler Haut deutlich geringer ist, als bei Menschen mit einer hellen Hautfarbe Auch konnten Unterschiede zwischen den Geschlechtern identifiziert werden, zu Ungunsten von Frauen Und diese Ungleichbehandlung beginnt bereits bei der Erstellung der Trainingsdaten, da die Instrumente zur Datenerfassung ebenfalls auf Personen mit bestimmten Merkmalen ausgelegt sind, wie z B die Lichttechnik bei Fotoaufnahmen, die häufig für Menschen mit heller Haut kalibriert wurde

Dies wirft natürlich vor allem im medizinischen Kontext bedeutende Fragen auf Ist es möglich, Patienten transparent zu machen, wenn der Arzt bei der Befundung von radiologischen Bildern von einer KI unterstützt wird? Wird die Entscheidungsfähigkeit des Arztes durch die KI-Unterstützung beeinflusst Das Fraunhofer benennt bereits für den gesamten Versorgungsprozess im Krankenhaus mögliche Anwendungsfälle, weist aber gleichzeitig darauf hin, dass „ganzheitliche Sicherheitskonzepte“ für den Einsatz von KI-Anwendungen in der Medizin erforderlich sind[6]

Die Rolle des Datenschutzes

Im Jahr 2019 beschloss die Datenschutzkonferenz die Hambacher Erklärung zur Künstlichen Intelligenz[7] Darin heißt es, dass „nicht alles, was technisch möglich und ökonomisch erwünscht ist, [ ] in der Realität umgesetzt werden darf“ Der Einsatz von selbstlernenden Systemen könne in massiver Weise in die Grundrechte der Menschen eingreifen und müsse daher gesetzlich reglementiert werden

Für die Entwicklung von KI-Systemen kommen daher die Anforderungen zum Datenschutz durch Technikgestaltung in besonderem Maße zum Tragen Hierzu formulieren die Datenschützer wesentliche Grundsätze, die ein KI-System einhalten müsse

1. **KI darf Menschen nicht zum Objekt machen:** Entscheidungen mit rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung dürfen nicht allein einer Maschine überlassen werden Betroffene hatten auch beim Einsatz von KI-Systemen den Anspruch auf das Eingreifen einer Person, auf die Darlegung ihres Standpunktes und die Anfechtung einer Entscheidung

2. **KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben:** KI-Systeme dürfen nur für verfassungsrechtlich legitimierten Zwecken eingesetzt werden, erweiterte oder neue Verarbeitungszwecke müssten mit dem ursprünglichen Erhebungszweck vereinbar sein

3. **KI muss transparent, nachvollziehbar und erklärbar sein:** Die Verarbeitung muss für die Betroffenen transparent sein, insbesondere hinsichtlich des Prozesses der Verarbeitung und über die verwendeten Trainingsdaten Nach der DSGVO ist dafür auch über die involvierte Logik ausreichend aufzuklären

4. **KI muss Diskriminierungen vermeiden:** Vor dem Einsatz von KI-Systemen müssen die Risiken für die Rechte und Freiheiten von Personen mit dem Ziel bewertet werden, auch verdeckte Diskriminierungen durch Gegenmaßnahmen zuverlässig auszuschließen Auch während der Anwendung von KI-Systemen muss eine entsprechende Risikoüberwachung erfolgen

5. **Für KI gilt der Grundsatz der Datenminimierung:** Die Verarbeitung personenbezogener Daten muss stets auf das notwendige Maß beschränkt sein Die Prüfung der Erforderlichkeit kann ergeben, dass die Verarbeitung vollständig anonymer Daten zur Erreichung des legitimen Zwecks ausreicht

6. **KI braucht Verantwortlichkeit:** Die Beteiligten beim Einsatz eines KI-Systems müssen die Verantwortlichkeit ermitteln und klar kommunizieren und jeweils die notwendigen Maßnahmen treffen, um die rechtmäßige Verarbeitung, die Betroffenenrechte, die Sicherheit der Verarbeitung und die Beherrschbarkeit des KI-Systems zu gewährleisten.

7. **KI benötigt technischen und organisatorischen Standard:** Für den datenschutzkonformen Einsatz von KI-Systemen gibt es gegenwärtig noch keine speziellen Standards oder detaillierte Anforderungen an technische und organisatorische Maßnahmen. Die Erkenntnisse in diesem Bereich zu mehren und Best-Practice-Beispiele zu entwickeln ist eine wichtige Aufgabe von Wirtschaft und Wissenschaft.

Seit 2021 versuchen die EU-Institutionen im sogenannten „AI Act" einen rechtlichen Rahmen zu erstellen, um KI-Systeme zu regulieren. Dort sollen unter anderem die Zuständigkeiten der Aufsichtsbehörden, die Notwendigkeit zum Auditing und der Zertifizierung von KI-Systemen, Produktverantwortung und die zwingende Kennzeichnung von maschinenunterstützten Produkten geregelt werden. Der Act verzögert sich allerdings weiter aufgrund eines festgefahrenen Streits, ob große Sprachmodelle generell als Hochrisiko-Technologie definiert werden sollten.

Fazit

Viele Einrichtungen der Gesundheitswirtschaft werden in der nahen Zukunft mit neuen Produkten konfrontiert sein, die KI-Systeme enthalten. Fachkräftemangel und hoher Wettbewerbsdruck verstärken die Erforderlichkeit zur Einführung solcher Lösungen. Es gilt daher, solche Lösungen nicht ohne gründliche Prüfung in die Prozesse zu integrieren. Die Beteiligung des Datenschutzbeauftragten dürfte hier unumgänglich sein, besonders da es bislang an einem verbindlichen und umfänglichen regulatorischen Rahmen mangelt.

David Große Dütting, Manager Curacon GmbH Wirtschaftsprüfungsgesellschaft.
David Große-Dütting ist als Manager in der Unternehmensberatung im Geschäftsfeld Datenschutz tätig und in vielen Unternehmen verschiedener Branchen als Datenschutzbeauftragter bestellt. Seine Schwerpunkte liegen in der Umsetzung der konfessionellen Datenschutzgesetze, der Bestandsaufnahme und Bewertung von Datenschutzmanagementsystemen sowie der datenschutzkonformen Gestaltung von Websites und Social Media Auftritten.

[1] https://www.fishbowlapp.com/insights/70-percent-of-workers-using-chatgpt-at-work-are-not-telling-their-boss/ [zuletzt aufgerufen am 24.03.2023]
[2] https://www.gatesnotes.com/The-Age-of-AI-Has-Begun [zuletzt aufgerufen am 24.03.2023]
[3] https://futureoflife.org/open-letter/pause-giant-ai-experiments/ [zuletzt aufgerufen am 06.04.2023]
[4] https://www.usenix.org/system/files/sec21-carlini-extracting.pdf [zuletzt aufgerufen am 06.04.2023]
[5] https://www.netflix.com/de/title/81328723 [zuletzt aufgerufen am 06.04.2023]
[6] https://www.iks.fraunhofer.de/de/themen/kuenstliche-intelligenz/kuenstliche-intelligenz-medizin.html [zuletzt aufgerufen am 06.04.2023]
[7] https://datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf [zuletzt aufgerufen am 06.04.2023].