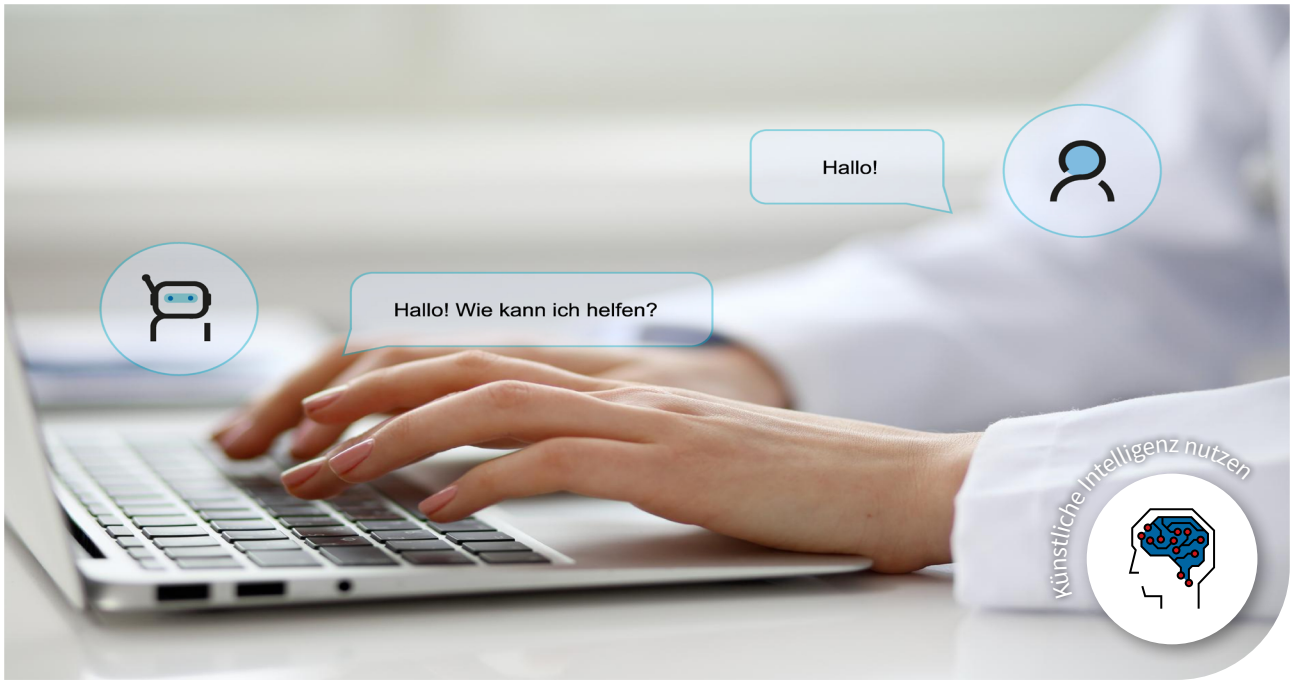
PRAXISTIPP

KI-Entscheidungen: Datenschutz und Erklärbarkeit im Fokus



Erklärbarkeit und Datenschutz

Der Einsatz von Systemen künstlicher Intelligenz (KI) kann viele Abläufe vereinfachen und den Aufwand zur Lösung von Problemen reduzieren. Kein Wunder, dass diese Technologie Einzug in die verschiedensten Bereiche gehalten hat. Von autonomen Fahrzeugen bis hin zu personalisierten Empfehlungssystemen beeinflusst KI bereits unseren Alltag. Jedoch birgt diese Technologie auch Herausforderungen, die nicht außer Acht gelassen werden dürfen. Insbesondere zwei Aspekte stehen dabei im Fokus: die Erklärbarkeit von KI-Entscheidungen und der Schutz der Privatsphäre durch entsprechende Datenschutzmaßnahmen.

In diesem Beispiel soll uns ein Chatbot als Anschauungsobjekt dienen, um zu zeigen, wie mit dem Problem erklärbarere KI-Entscheidungen umgegangen werden kann. Dabei nimmt der Chatbot, eingebunden in die Homepage eines Unternehmens, Kundenanfragen entgegen und vergibt Termine.

Zusammenspiel von Datenschutz und Erklärbarkeit von KI

Beim Entgegennehmen von Kundenanfragen und die Terminvereinbarungen verarbeitet das KI-System personenbezogene Daten. Daher ist die Datenschutzgrundverordnung (DSGVO) für diese Verarbeitungsvorgänge anwendbar.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Aus dieser stehen dem „Betroffenen“ verschiedene Rechte zu. Betroffen ist, wessen personenbezogene Daten verarbeitet werden (Art. 4 Nr. 1 DSGVO). Zu den Rechten zählt unter anderem das Auskunftsrecht aus Art. 15 DSGVO. Nach diesem müssen Betroffenen verschiedene Informationen mitgeteilt werden. Beispielsweise, welche Kategorien personenbezogener Daten für welche Zwecke verarbeitet werden, aber auch wie lange die Daten gespeichert werden.

Für unser Beispiel heißt das, dass die Kundendaten zum Zweck der Terminvereinbarung für die jeweilige Leistung erhoben werden, bis der Termin abgeschlossen ist.

Einen weiteren Auskunftsanspruch des Betroffenen regelt Art. 15 Abs. 1 lit. h) DSGVO. Nach diesem steht Betroffenen eine aussagekräftige Information hinsichtlich der involvierten Logik und der angestrebten Auswirkung einer automatisiert getroffenen Entscheidung zu.

Betroffene können Informationen über die grundlegende Funktionsweise des Algorithmus verlangen. Nun kommt jedoch die komplexe Funktion von modernen KI-Systemen zum Tragen. Sie basieren in der Regel auf sogenannten tiefen neuronalen Netzen, die in einer Vielzahl von Schichten Ableitungen über die Eingaben treffen und daraus wiederum andere Informationen ziehen. Häufig sind diese Netze so ausgestaltet, dass sie wiederum weiter aus dem „lernen“, was sie verarbeiten, ihre Parameter sich also konstant verändern.

Dieser hohe Grad an Komplexität führt zum sogenannten „black-box“-Problem. Kurz gesagt: Es ist eigentlich nicht zu erklären, wie die KI zu ihrem Ergebnis gelangt. Eine Offenlegung der genauen Funktionalität des KI-Systems ist also gar nicht möglich.

Jedoch wäre bei einem „normalen“ Algorithmus das Offenlegen der Algorithmus-Formel auch nicht notwendig. Die Verpflichtung zu einer nachvollziehbaren Information ist keine zu einer nachrechenbaren Information.

Für das Auskunftsverlangen einer betroffenen Person genügt es in der Regel, die grundsätzlichen Funktionen und wichtigsten Parameter, die der Algorithmus benötigt, zu erklären. Noch wichtiger für unser Beispiel ist jedoch der Punkt, dass sich diese Erklärung über die Funktionalität des Algorithmus nur auf automatisierte Entscheidungen im Sinne des Art. 22 DSGVO bezieht. Also Entscheidungen mit rechtlicher Wirkung oder einer ähnlich erheblichen Beeinträchtigung. Die einfache Terminvereinbarung oder die Beantwortung von Fragen im Kundensupport ist jedoch keine solche Entscheidung. Darum ist eine so weitgehende Informationsverpflichtung nicht gegeben.

Fazit

Die Grundsätze des Datenschutzrechts gelten auch für Systeme künstlicher Intelligenz und verpflichten die Verantwortlichen zu einem sorgsamen Umgang mit personenbezogenen Daten. Dabei sind auch die Rechte der Betroffenen Personen zu wahren und Auskunft über die verarbeiteten Daten zu geben. Wie genau die Verarbeitung durch die KI erfolgt, muss jedoch nicht erklärt werden, zumal dies technisch auch nicht möglich ist. Vielmehr reicht es in besonderen Fällen – wenn eine automatisierte Entscheidung getroffen wird – die grundsätzliche Funktion des Algorithmus sowie die maßgeblichen Parameter zu offenbaren.

Mittelstand-Digital Zentrum Chemnitz
c/o Technische Universität Chemnitz
09125 Chemnitz
0371 531-19935
info@digitalzentrum-chemnitz.de

Stephan Kunitz
0371 531 37216
stephan.kunitz@digitalzentrum-chemnitz.de

digitalzentrum-chemnitz.de