



VERWENDUNG VON AUF KI-SYSTEMEN BASIERENDEN CHATBOTS

Informationen zum Datenschutz | September 2024

English version

Einleitung

Die Einbindung und Nutzung von KI-Tools in den Arbeitsalltag sowie das Angebot eigener KI-Anwendungen, insbesondere Chatbots, gewinnt für Unternehmen zunehmend an Bedeutung. Dies betrifft unter anderem Übersetzungstools oder Anwendungen wie ChatGPT, mittels derer sich Fragen beantworten oder Texte erzeugen lassen. Werden im Rahmen der Nutzung der jeweiligen Anwendung personenbezogene Daten verarbeitet, müssen hierbei neben anderen rechtlichen Anforderungen vor allem auch die datenschutzrechtlichen Vorgaben der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) sowie die Regelungen der neuen KI-Verordnung eingehalten werden. Letztere ist am 12. Juli 2024 im Amtsblatt der EU veröffentlicht worden und am 1. August 2024 in Kraft getreten. Die meisten Regelungen des neuen Rechtsaktes finden ab dem 2. August 2026 Anwendung. Verschiedene Vorgaben sind aber bereits ab dem 2. Februar 2025 bzw. dem 2. August 2025 zu beachten.

Der Begriff der „KI-Systeme“ ist in Art. 3 Nr. 1 KI-Verordnung legal-definiert. Demnach ist ein KI-System ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.

Eigene Nutzung von Chatbots

Sollen personenbezogene Daten in einen Chatbot oder ein anderes KI-Tool eingegeben und durch dieses verarbeitet werden, bedarf es einer Rechtsgrundlage für die hierbei stattfindenden Datenverarbeitungsprozesse. Es gilt insoweit der in Art. 6 DSGVO verankerte datenschutzrechtliche Grundsatz des Verbots mit Erlaubnisvorbehalt.

Zur Rechtfertigung der Datenverarbeitungsprozesse kommt vor allem die Einwilligung des von der Datenverarbeitung Betroffenen nach Art. 6 Abs. 1 S. 1 lit. a) DSGVO in Betracht, die, um wirksam zu sein, allerdings verschiedenen Anforderungen gerecht werden muss. Schwierigkeiten können sich insoweit hinsichtlich des Merkmals „in informierter Weise“ ergeben, da die transparente Information der Betroffenen das Unternehmen, das die Daten in das Tool eingeben möchte und insoweit informationspflichtig ist, durchaus vor Herausforderungen stellen kann. Dies liegt mitunter daran, dass

es für das Unternehmen in vielen Fällen angesichts der Komplexität der Tools und der Zurückhaltung der Tool-Anbieter, die konkreten Datenverarbeitungsprozesse und Mechanismen der Anwendung offenzulegen, nicht einfach sein dürfte, die erforderlichen Informationen zusammenzustellen.

Kommt ein Unternehmen im Rahmen der geforderten Interessenabwägung zu dem Ergebnis, dass die eigenen Interessen an dem Einsatz des KI-Tools die Interessen, Grundrechte und Grundfreiheiten des Betroffenen überwiegen, kommt vom Grundsatz her im Einzelfall auch das berechtigte Interesse des Unternehmens gem. Art. 6 Abs. 1 S. 1 lit. f) DSGVO als Rechtsgrundlage in Betracht. Es ist jedoch darauf zu achten, dass es grundsätzlich einer Entscheidung im Einzelfall bedarf und ein überwiegendes Interesse aufgrund der mit der Datenverarbeitung verbundenen Risiken nicht vorschnell angenommen werden darf. Beziehen sich die Datenverarbeitungsprozesse auf Mitarbeiterdaten, kann auch an eine Betriebsvereinbarung gedacht werden.

Einige Anbieter von KI-Anwendungen bieten zudem den Abschluss einer Vereinbarung zur Auftragsverarbeitung an. Wird der Anbieter des Chatbots als Auftragsverarbeiter für das verantwortliche Unternehmen tätig und die Datenverarbeitung über eine entsprechende Vereinbarung i.S.v. Art. 28 DSGVO abgesichert, kommt auch insoweit Art. 6 Abs. 1 S. 1 lit. f) DSGVO i.V.m. Art. 28 DSGVO als Rechtsgrundlage in Betracht. Liegt hingegen keine Einwilligung der Betroffenen vor und fehlt es auch im Übrigen an einer Rechtsgrundlage, muss eine Eingabe von personenbezogenen Daten in den Chatbot mangels Rechtsgrundlage ausscheiden. Es ist in diesem Fall aber denkbar, anonymisierte Daten in das Tool einzugeben, soweit gewährleistet werden kann, dass sich hieraus tatsächlich keine Rückschlüsse auf eine natürliche Person ergeben.

Darüber hinaus müssen die Betroffenen nach Art. 13 DSGVO über die Datenverarbeitung informiert werden. Es ergeben sich insoweit vergleichbare Schwierigkeiten wie hinsichtlich der Informiertheit der Einwilligung.

Um den ordnungsgemäßen Umgang mit Chatbots unternehmensintern sicherzustellen, bietet sich die Erstellung einer Richtlinie zum ordnungsgemäßen Umgang mit KI-Tools an. In dieser können etwa die nachfolgenden Aspekte geregelt werden:

- Welche Anwendungen dürfen genutzt werden?
- Welche Informationen dürfen in die Anwendungen eingegeben werden?
- Zu welchen Zwecken dürfen die Anwendungen genutzt werden?
- Sind von KI-Anwendungen erzeugte Ergebnisse gesondert zu kennzeichnen?
- Wie und von wem werden die erzeugten Ergebnisse überprüft?
- Wie wird dem erhöhten Gefahrenpotential begegnet?
- Wie werden die Vorgänge dokumentiert?

Angebot eines Chatbots

Bietet ein Unternehmen selbst einen Chatbot an, der etwa Fragen zu Produkten des Unternehmens oder Ansprechpartnern beantwortet, ist darauf zu achten, dass das Tool nur dann mit personenbezogenen Daten trainiert wird, wenn insoweit eine Rechtsgrundlage vorliegt. Gleiches gilt für die Ausgabe von Arbeitsergebnissen, die personenbezogene Daten enthalten.

Neben etwaigen datenschutzrechtlichen Informationspflichten bestehen zudem Transparenzpflichten nach der KI-Verordnung. Die Nutzer des Tools sind nach Art. 50 KI-Verordnung insbesondere über den Umstand aufzuklären, dass sie mit einem KI-Tool interagieren, soweit dies aufgrund der Umstände und des Kontextes der Nutzung nicht ohnehin aus Sicht einer angemessen informierten, aufmerksamen und verständigen natürlichen Person offensichtlich ist. Daneben haben Anbieter von KI-Systemen unter Umständen verschiedene Überwachungs-, Dokumentations- und Meldepflichten einzuhalten.

Entscheidungen durch KI-Tools

Handelt es sich bei dem verwendeten oder angebotenen Tool nicht ausschließlich um einen Chatbot, sondern werden auch Entscheidungen durch das Tool getroffen – etwa über den Abschluss eines

Vertrages – sind darüber hinaus weitergehende Transparenzpflichten und Anforderungen, die die KI-Verordnung an Hochrisiko-KI-Systeme stellt, zu beachten. Diese sind im konkreten Einzelfall näher zu bestimmen.

Aus datenschutzrechtlicher Sicht sind zudem die Vorschrift des Art. 22 DSGVO und die insoweit bestehenden Vorgaben für automatisierte Einzelentscheidungen zu beachten. Darüber hinaus kann die Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich werden.

Fazit

Bei der Nutzung von auf KI-Systemen basierenden Chatbots und sonstigen KI-Anwendungen müssen die allgemeinen datenschutzrechtlichen Vorgaben der DSGVO und des BDSG sowie die Vorgaben der neuen KI-Verordnung beachtet werden. Dies betrifft vor allem den Grundsatz des Verbots mit Erlaubnisvorbehalt und das hieraus resultierende Erfordernis einer Rechtsgrundlage für jede im Zusammenhang mit der Verwendung der KI-Anwendung erfolgende Verarbeitung personenbezogener Daten sowie die verschiedenen Informations- und Transparenzpflichten. Gleiches gilt, wenn entsprechende Tools Kunden und Interessenten etwa über die Homepage des Unternehmens zur Nutzung angeboten werden. Neben der rechtlichen Pflicht zur Offenlegung des Einsatzes von KI-Tools, empfiehlt es sich auch im Übrigen, eine KI-Nutzung offenzulegen, um den Vorwurf der Irreführung oder Intransparenz zu vermeiden. Welche Pflichten sich im Einzelnen ergeben, richtet sich nach dem Funktionsumfang des jeweiligen Tools und ist im Einzelfall zu bestimmen. Um den ordnungsgemäßen Umgang mit KI-Anwendungen im Unternehmen sicherzustellen, bietet sich die Erstellung einer KI-Richtlinie an, innerhalb derer unterschiedliche Aspekte verbindlich geregelt werden können. Gerne unterstützen wir Sie bei der konkreten Ausgestaltung.

Christina Prowald



Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin
T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net