Universität Regensburg

Datenschutzbeauftragter

Ass. jur. Susanne Stingl
Dienstgebäude "Altes Finanzamt"
Raum 135, 1. OG.
Landshuter Straße 4
93047 Regensburg
Telefon 0941 943-5376
Fax 0941 943-5369
E-Mail dsb@ur.de

7. Merkblatt der Datenschutzbeauftragten

Stand: 22.02.2024

Datenschutz bei Nutzung von Künstlicher Intelligenz (KI)

Durch den Hype um den Chatbot ChatGPT ist das Thema künstliche Intelligenz in den Fokus gerückt. Diese bietet vielfältige neue Möglichkeiten zur Arbeitserleichterung. Gleichzeitig stammen viele der Produkte aus den USA oder anderen Ländern außerhalb der EU, so dass nicht sichergestellt ist, dass europäische Standards eingehalten werden. Dieses Merkblatt soll Sie beim Einsatz von KI in Verwaltung und Lehre im Hinblick auf den Datenschutz unterstützen. Da aktuell ChatGPT im Fokus steht und am meisten genutzt wird, wird dieses häufig als Beispiel herangezogen, jedoch auch allgemeine Aussagen zur Nutzung von KI getroffen.

Problematik und Risiken

Der Einsatz von KI ist nicht per se datenschutzrechtlich problematisch. Wie bei allen Tools kommt es darauf an, wie es eingesetzt wird.

Trainingsdaten

Das höchste Risiko bei dem Einsatz von KI aus datenschutzrechtlicher Perspektive liegt in dem Schulungsdatensatz der jeweiligen KI. Denn aufgrund komplexer neuronaler Netze kann derzeit niemand zuverlässig kontrollieren, welche Daten durch die KI ausgegeben werden. So kann es passieren, dass Daten, die man in die KI eingibt, Dritten ausgegeben werden, da sie regelmäßig zur Weiterentwicklung der KI genutzt werden. Wenn es sich dabei um personenbezogene Daten handelt und es keine Rechtsgrundlage gibt, stellt dies einen Verstoß dar. Insbesondere bei kostenlosen Produkten werden die eingegebenen Daten regelmäßig auch zu Trainingszwecken für die KI genutzt.

Nutzendendaten

Regelmäßig ist es erforderlich, einen Account für die Nutzung der Produkte anzulegen. Teilweise muss neben der E-Mailadresse auch eine Mobilfunknummer zur Verifizierung angegeben werden. ChatGPT beispielsweise behält sich vor, diese Daten zu nutzen, ohne explizit darüber zu informieren, wie diese Nutzung erfolgt. ChatGPT kann somit die Aktivität der Nutzenden tracken und ggf. mit anderen Daten verbinden.

Berufs- und Geschäftsgeheimnisse

Nicht nur im Bezug auf den Schutz des Persönlichkeitsrechtes von natürlichen Personen bestehen Gefahren. Werden beispielsweise Daten, die unter § 203 StGB fallen (bestimmte Daten, die einem als Amtsträger oder Arzt bekannt wurden), in ChatGPT eingegeben, kann dies sogar strafrechtliche Konsequenzen haben.

Gerade im Bereich der Forschung kann die Eingabe von Daten noch nicht veröffentlichter Forschungsdaten oder vertraulicher Unternehmensdaten zu Folgeproblemen führen. Alle Daten, die in ChatGPT eingegeben werden, stehen dem Unternehmen OpenAI zur Verfügung und können von diesem für eigene Zwecke genutzt werden.

Erforderliche Verträge

Eine weitere Hürde stellt eine Vertragsbeziehung zwischen der UR und dem KI-Anbieter da. Wenn die UR aktiv einen Dienst als Arbeitsmittel anbieten will, so ist mit dem Anbieter ein entsprechender Vertrag zu schließen. Gerade bei amerikanischen Tech-Konzernen hat sich in der Vergangenheit gezeigt, dass diese teilweise die europarechtlich vorgeschriebenen Vertragsbedingungen nicht in die Verträge aufnehmen und umsetzen wollen.

„Halluzinieren"

Neben der datenschutzrechtlichen Problematik sollte man stets beachten, dass die KI in der derzeitigen Form, nicht im Sinne eines Menschen „denken" kann. Sie stellt lediglich anhand von Wahrscheinlichkeiten Ergebnisse zusammen. Als Wissensquelle sollte man KI daher nicht nutzen. Gerade ChatGPT ist bekannt dafür, häufig Fakten zu erfinden, die zwar plausibel wirken, aber nicht wahr sind. Zudem bestehen die Schulungsdaten u.a. aus einer Masse an öffentlichen Internetdaten, die zum einen unwahr sein können, zum anderen aber verschiedenen Verzerrungen und Diskriminierungsmechanismen unterliegen können.

Handlungsoptionen

Oben gesagtes bedeutet jedoch nicht, dass man KI oder im speziellen ChatGPT gar nicht nutzen kann.

Grundsätzlich ist die Eingabe von Daten in ChatGPT oder ähnliche Produkte damit zu vergleichen, Daten zu veröffentlichen, auch wenn sie im Gegensatz zu einer Website nicht unmittelbar weltweit abrufbar sind. **Als Faustregel kann man sich daher merken: Nur Daten eingeben, die man auch im Internet veröffentlichen würde und darf.**

Daten ohne Personenbezug

Aus datenschutzrechtlicher Sicht unproblematisch ist die Eingabe von Daten ohne Personenbezug. ChatGPT selbst weist bei der Anmeldung und in seinen Nutzungsbedingungen darauf hin, dass keine personenbezogenen oder sensiblen Daten eigegeben werden dürfen. Solange der Prompt nur allgemeine Fragestellungen und Anweisungen erhält, die keinen Personenbezug aufweisen oder geheimhaltungswürdige Daten enthält, liegt kein Verstoß vor. So kann ChatGPT zum Beispiel genutzt werden, um Webseitentexte zu optimieren, öffentliche Reden oder Artikel zu schreiben. Öffentlich zugängliche Texte können zusammengefasst werden.

Nutzendentracking

Grundsätzlich sollte man Mitarbeitenden oder Studierenden die Nutzung von Tools, die ihr Verhalten tracken, nicht vorschreiben. Wenn man wünscht, dass das Tool eingesetzt werden darf, sollte man es den Nutzenden immer freistellen und Alternativen anbieten, oder Vorkehrungen treffen, dass die Daten nicht auf eine konkrete Person zurückzuführen sind, wie beispielsweise die Anmeldung über eine Funktionsemailadresse oder anonyme Mailadresse, sowie die Nutzung eines Diensttelefons. Die Nutzenden sollten sich nicht über ein Google- oder Microsoftkonto oder ähnlichem anmelden, da hier Daten zusätzlich verknüpft werden.

Wo immer möglich, sollten die Chathistorie und die Nutzung als Trainingsdaten deaktiviert werden.

Lizenzmodelle, Schnittstellen und Co.

KI-Tools stecken noch in den Kinderschuhen. Wie bei anderen Entwicklungen auch, z.B. Videokonferenztools, müssen vor allem außereuropäische Anbieter zur Einhaltung der DSGVO geführt werden. Es ist absehbar, dass es von verschiedenen Tools Lizenz- und Bezahlmodelle geben wird oder es diese zum Teil auch schon gibt, bei denen zum einen die erforderlichen datenschutzrechtlichen Verträge geschlossen werden, zum anderen die Daten nur für vorgesehene und abgestimmte Zwecke verarbeitet werden. Beispielsweise kann geregelt werden, dass die Eingabedaten nicht für Trainingszwecke genutzt werden oder das Tool auf einer eigenen Instanz betrieben wird, so dass die Daten nicht an Dritte gehen, gleichzeitig aber zum Training genutzt werden können. Auch kann geregelt werden, dass die Nutzenden nicht getrackt werden. Einige Anbieter stellen auch eine Zwischeninstanz zur Verfügung, so dass die Nutzendendaten nicht an den KI-Betreiber weitergegeben werden.

Wo möglich und erforderlich sollte ein Auftragsverarbeitungsvertrag mit den Anbietern geschlossen werden, in welchem die Nutzung für eigene Zwecke und Trainingszwecke explizit ausgeschlossen wird. Bei einigen Tools besteht die Möglichkeit, diese mittels API-Schnittstelle in die eigene Website einzubinden. Hierfür wird ein Auftragsverarbeitungsvertrag angeboten, über den die Daten nicht für eigene Zwecke des KI-Anbieters genutzt werden. Bei der Einbindung von Tools auf der eigenen Webseite ist jedoch immer zu beachten, dass die Nutzenden gem. Art. 13 DSGVO über die Verarbeitung Ihrer Daten informiert werden.

Eigene Entwicklungen

Gerade bei der Zusammenarbeit mit großen Unternehmen, in Verbünden und Forschungsprojekten besteht die Option, eigene KI-basierte Tools zu entwickeln, bei denen man die Kontrolle über die Datenverarbeitung hat und die DSGVO von Anfang an berücksichtigen kann. Diese Gelegenheit sollte man nach Möglichkeit nicht verstreichen lassen.

Bei Fragen zum Thema wenden Sie sich gern an dsb@ur.de.