Neues zum Einsatz von KI-Modellen

Künstliche Intelligenz (KI) spielt eine immer größere Rolle, was auch zunehmend rechtliche Fragen aufwirft. Mitte Juli wurde die lange diskutierte KI-Verordnung der EU veröffentlicht, die Anfang August in Kraft getreten ist. Sie stellt erstmals einen Rechtsrahmen für den Einsatz von KI-Systemen auf. Die meisten Pflichten werden in zwei Jahren unmittelbar gelten. In einem kürzlich veröffentlichten Diskussionspapier des Hamburgischen Datenschutzbeauftragten wird darüber hinaus das Verhältnis von Datenschutz und Large Language Models (LLMs) erörtert, wie es z.B. ChatGPT zugrunde liegt. Das soll Unternehmen bei der datenschutzkonformen Nutzung von KI-Systemen, die LLMs einsetzen, unterstützen. Wir fassen die wichtigsten Entwicklungen für Sie als Datenschützer in unserem Artikel zusammen.

Hamburger Thesen zum Personenbezug in LLMs

Der Hamburgische Beauftragte für den Datenschutz und die Informationsfreiheit (HmbBfDI) hat sich in einem Diskussionspapier mit dem Verhältnis der DSGVO zu Large Language Models (LLMs) beschäftigt. Ein LLM ist eine Komponente eines KI-Modells, die Sprachen verstehen, verarbeiten und generieren kann. Das bekannteste Beispiel für ein KI-Modell, welche ein LLM beinhaltet, ist ChatGPT. Bei der Nutzung eines LLMs können nicht nur im eigenen Prompt, den der Nutzer eingibt, sondern auch im sog. Output Angaben über natürliche Personen enthalten sein, insbesondere, wenn Nutzer das System explizit danach fragen. Das warf beim HmbBfDI die Frage auf, ob LLMs personenbezogene Daten speichern und daher quasi „aus sich heraus“ im Output produzieren. Der HmbBfDI sieht dies differenziert:

- **In LLMs werden keine personenbezogenen Daten gespeichert**

  Trainingsdaten für LLMs und auch Inputs (sog. Prompts) können personenbezogene Daten enthalten. Die LLMs selbst speichern nach HmbBfDI aber keine personenbezogenen

Daten. Dies bedeutet, dass im System selbst die beim Training verwendeten personenbezogenen Daten nicht mehr als solche vorhanden sind, sie haben lediglich zur Entwicklung der entsprechenden Gewichte und Tokens geführt.

Wer ein LLM speichert und hostet, verarbeitet daher auch noch keine personenbezogenen Daten i.S.v. Art. 4 Nr. 2 DSGVO. Das LLM ist insofern nur „Tool", wie eine Software. Personenbezogene Daten werden mit diesem erst und nur dann verarbeitet, wenn es mit solchen trainiert wird oder aber im entsprechenden Input oder Output.

- **Ein LLM kann nicht selbst Gegenstand von Betroffenenrechten sein**

  Mangels Speicherung personenbezogener Daten im LLM, können die Betroffenenrechte der DSGVO auch nicht das LLM selbst zum Gegenstand haben. Sie können sich aber auf Trainingsdaten, Input oder Output eines KI-Systems, das ein LLM beinhaltet, beziehen. Das ist dann auch maßgeblich für die Person, der gegenüber die Betroffenenrechte geltend gemacht werden, ähnlich der bei Software bekannten Differenzierung zwischen Hersteller und Anwender der Software.

- **Training mit personenbezogenen Daten nur im Rahmen der DSGVO**

  LLMs dürfen nur im Rahmen des Datenschutzrechts mit personenbezogenen Daten trainiert werden. Auch die Betroffenenrechte müssen dabei selbstverständlich beachtet werden.

  Allerdings wirkt sich ein Datenschutzverstoß beim Training des LLMs nicht auf die Rechtmäßigkeit seines Einsatzes aus, wenn mit dem HmbBfDi davon ausgegangen wird, dass das LLM selber keine personenbezogenen Daten speichert. Einem Unternehmen, welches Daten mit KI-Systemen verarbeitet, wird ein etwaiger Datenschutzverstoß beim Training des integrierten LLMs dann auch nicht zugerechnet. Allein der Entwickler des LLMs ist für das rechtmäßige Training seines Modells verantwortlich. Dies entlastet alle Nutzer von ChatGPT & Co. enorm, die immer wieder

datenschutzrechtlichen Bedenken hinsichtlich ihres Trainings ausgesetzt sind.

Möchte ein Unternehmen jedoch selbst das LLM nachtrainieren, sollte darauf geachtet werden, dass personenbezogenen Daten nur unter strenger Einhaltung des Datenschutzrechts dafür verwendet werden.

KI-Verordnung der EU veröffentlicht

Die erste umfassende KI-Risikoregulierung kommt aus der EU: Am 12.07.2024 ist die Verordnung über künstliche Intelligenz (Verordnung (EU) 2024/1689; im Folgenden: „KI-Verordnung“) im Amtsblatt der EU veröffentlicht worden. Die KI-Verordnung ist damit am 01.08.2024 in Kraft, der Großteil ihrer Regelung wird ab dem 02.08.2026 unmittelbar in allen EU-Mitgliedstaaten gelten.

Im Wesentlichen wird damit ein Rechtsrahmen für eine risikogerechte Entwicklung, Inverkehrbringen und Anwendung von KI-Systemen geschaffen, der die Werte der EU schützt und die Grundrechte der Unionsbürger wahrt. Gleichzeitig sollen Innovationen durch den freien Verkehr KI-gestützter Waren und Dienstleistungen in der EU gefördert werden. Dafür werden mit der KI-Verordnung weder das Datenschutzrecht, das Urheberrecht oder das Haftungsrecht geregelt. Vielmehr bringt die KI-Verordnung eine risikoangemessen KI-Governance-Pflicht für alle Entwickler und Anwender von KI-gestützten Systemen.

Die wesentlichen Elemente der KI-Verordnung lassen sich wie folgt zusammenfassen:

- **Risikoklassifizierung von KI-Systemen**

  Inakzeptable KI-Systeme werden verboten. Dies betrifft Anwendungen wir etwa das „Social Scoring“, bei dem Personen auf Grundlage ihres Sozialverhaltens bewertet werden. Ebenso verboten wird die Erstellung von Datenbanken zur Gesichtserkennung durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet.

  Andere Systeme werden als Hochrisiko-KI-Systeme eingestuft, beispielsweise KI in Funkanlagen oder für KI für Personalentscheidungen. Sie unterliegen weitreichenden

Risikoüberprüfungen, Dokumentations- und Transparenzpflichten, flankiert durch Anforderungen an eine umfassende KI-Governance im Unternehmen. Bei ihrer Entwicklung und ihrem Einsatz im Unternehmen muss u.a. besonders auf die Qualität der verwendeten Daten, Cybersicherheit und Risikomanagement geachtet werden. Auch Anwender unterfallen weitreichenden Informationspflichten ggü. allen Betroffenen.

Dagegen fallen KI-Systeme, die nur mit einem mittleren oder geringen Risiko verbunden sind, nur unter wenig strenge Vorgaben der KI-Verordnung. Dies betrifft etwa Kennzeichnungspflichten für Deepfakes und KI, die zur Interaktion mit Menschen genutzt wird (Chatbots & Co.).

- **Einbeziehung von Datenschutzaufsichtsbehörden und Aufsicht**

  Außerdem erhalten Datenschutzaufsichtsbehörden besondere Befugnisse, wie den Zugriff zu Dokumenten, die zur Erfüllung der Aufgaben nach der KI-Verordnung erforderlich sind. Gewisse Anbieter von Hochrisiko-KI-Systemen müssen diese registrieren. Werden bei der Entwicklung und dem Training von KI in sog. Reallaboren personenbezogene Daten verarbeitet, sollen die Datenschutzaufsichtsbehörden ebenfalls einbezogen werden.

  Die Aufsicht über (Hochrisiko-)KI-Systeme wird der EU Kommission und den zuständigen Marktüberwachungsbehörden übertragen. Auf nationaler Ebene müssen die EU-Staaten jeweils einen sog. „Single-Point-of-Contact“ benennen, der als zentrale Anlaufstelle in Bezug auf KI u.a. Beschwerden und Meldungen entgegennehmen soll.

  Erarbeitet wird derzeit auch eine entsprechende Behördenstruktur mit einem AI Office auf EU-Ebene und nationalen Behörden. Einige Unternehmen müssen zudem AI Officer benennen.

KI-Governance-Programme

Verstöße gegen die KI-Verordnung sind mit enormen Bußgeldern belegt. Es ist daher angezeigt, zeitnah eine Betroffenheitsanalyse einzuleiten, wenn KI im Unternehmen entwickelt oder eingesetzt wird. Im ersten Zugriff helfen hierbei AI Act Compliance Checker, die aber oftmals zu pauschal sind, um wirkliche Hilfestellung zu bieten. In diesem Fall sollte intern eine zuständige Stelle geschaffen werden, die die Relevanzprüfung aufnimmt – wir unterstützen dabei gerne mit Workshops bis hin zur Gutachtenerstellung oder – oft sehr effektiv – der Prozessbegleitung insgesamt.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Philipp Schoel
+49(0)221 65065-200
philipp.schoel@loschelder.de

Dennis Pethke, LL.M.
+49(0)221 65065-337
dennis.pethke@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de