07 Betroffenenrechte bei KI: Auskunft und Co. vorbereiten

Die Rechte der betroffenen Personen stellen eine bedeutende Säule des Datenschutzes dar. Daher ergeben sich auch bei KI-Systemen für Betroffene Fragen wie „Welche Daten werden von mir wozu verarbeitet?“, „Werde ich überhaupt darüber informiert, dass KI bei meinen Daten zur Verarbeitung verwendet wird?“ und „Können meine Daten aus einer KI auch wieder gelöscht werden?“ Für Unternehmen können derartige Anforderungen an die Datenschutzorganisation gerade bei Einsatz von innovativen Technologien mitunter noch zur Herausforderung werden – es sei denn, die zuständige Aufsichtsbehörde berät dazu.

• • • lda.bayern.de/ki07

08 Zukunft der KI: Optimismus statt Sorge vor der Superintelligenz

KI hat das Potential, unsere Wirtschaft und Gesellschaft maßgeblich und nachhaltig zu beeinflussen. Leistungsstarke KI kann mehr Wertschöpfung und Wohlstand generieren, solange diese nicht zu unredlichen oder kriminellen Zwecken eingesetzt wird. Aus diesem Grund bedarf Innovation einer Regulierung, die offen für Neues, kompetent in der Sache und schlank bei der Bürokratie ist. Das Bayerische Landesamt für Datenschutzaufsicht ist bestrebt, weiterhin einen wesentlichen Beitrag bei der KI-Regulierung durch die Sicherstellung des Grundrechtsschutzes in Bayern zu leisten. Feedback zum bestehendem KI-Informationsangebot ist daher willkommen.

• • • lda.bayern.de/ki08

Quo vadis, KI?

Mit Datenschutz KI begleiten

Unaufhaltsam auf dem Weg nach oben? Im letzten Jahrzehnt gab es bei künstlichen neuronalen Netzen einen derartig rasanten Entwicklungssprung, dass sie heutzutage nahezu synonym zu KI verwendet werden. Mit den beeindruckenden Möglichkeiten von Text- und Bildgenerierung ist KI in jüngster Zeit schon Mainstream geworden und so auch in viele bayerische Betriebe eingezogen. Beim Einsatz von KI stellen sich viele datenschutzrelevante Fragen, etwa zur Personenbeziehbarkeit von KI-Daten oder zum Durchführen von dazugehörigen Datenschutzfolgenabschätzungen. Die im Flyer enthaltenen Informationen dienen als erste Ansatzpunkte für Maßnahmen zum datenschutzkonformen Einsatz von KI. Auf der BayLDA-Website sind weitere hilfreiche Tipps und Links zu finden sowie eine Checkliste, die Anforderungen an die Entwicklung und den Einsatz von Anwendungen der Kategorie KI darstellt.

KI Next Level
Mehr Vertrauen mit Datenschutz
www.lda.bayern.de/ki

Herausgeber

Bayerisches Landesamt für Datenschutzaufsicht
Cybersicherheit und technischer Datenschutz
Promenade 18
91522 Ansbach

Bayerisches Landesamt für Datenschutzaufsicht

Künstliche Intelligenz

Mehr Vertrauen mit Datenschutz

Next-Level-Bausteine für KI:
Mit Datenschutz Vertrauenswürdigkeit gewinnen und KI zukunftssicher gestalten

01 KI rechtskonform einsetzen: Grundlagen kennen & meistern

KI für Menschen bedeutet meist zwangsläufig auch die Verarbeitung personenbezogener Daten. Werden solche Daten beim Einsatz von KI verarbeitet, so ist frühzeitig an die datenschutzrechtlichen Aspekte zu denken. Die Prüfung, welche Rechtsgrundlage dafür verwendet werden kann, gehört zum Einmaleins des Umgangs mit personenbezogenen Daten – sei es beim Training eines KI-Systems oder bei Nutzung einer KI-Anwendung mittels Weboberfläche. Mit einem Eintrag in das ohnehin schon vorhandene Verarbeitungsverzeichnis ist der Grundstein für einen datenschutzkonformen KI-Einsatz schnell und unbürokratisch gelegt.

lda.bayern.de/ki01

02 Datenschutzfolgenabschätzung: Hochrisiko-KI in Schach halten

KI-Systeme liefern in der Anwendung mitunter fantastische Ergebnisse. In manchen Szenarien, wie bspw. bei einer Verarbeitung von Gesundheitsdaten oder beim Umgang mit Personaldaten, können sich durch den KI-Einsatz allerdings hohe Risiken für die betroffenen Personen ergeben. Mit dem richtigen Datenschutzwerkzeug kann daher rechtzeitig gegengesteuert werden: Die Datenschutzfolgenabschätzung ist nicht nur das (verpflichtende) Mittel der Wahl, hohen Risiken strukturiert und nachweislich in den Griff zu bekommen – sie dient auch dazu, mehr Vertrauen in den eigenen KI-Einsatz aufzubauen.

lda.bayern.de/ki02

03 KI-as-a-Service: Datenschutz nicht automatisch inbegriffen

Wer auf einen „KI-as-a-Service"-Dienstleister zurückgreift, etwa um sich ein kostenintensives Trainieren von KI-Modellen zu sparen, muss die Besonderheiten der Auftragsverarbeitung und ggf. eines Drittlandstransfers berücksichtigen. Bei Nutzung von US-Dienstleistern besteht mit dem EU-US-Datenschutzframework mittlerweile ein einfach zu nutzendendes Rechtsinstrument. Problematisch kann es allerdings werden, wenn der Dienstleister Eingabedaten ungeregelt für eigene Zwecke verwendet (z. B. zur Produktverbesserung). Vertrauen samt Kontrolle sind daher nicht nur bei der Auswahl der KI erforderlich, sondern auch bei der des Dienstleisters.

lda.bayern.de/ki03

04 Besonderer Fokus Datenschutz: KI-Schutzziele kennen

Datenschutzrisiken für die Rechte und Freiheiten natürlicher Personen bei KI-Einsatz ergeben sich, wenn KI-spezifische Schutzziele nicht vollständig erfüllt werden. Beispiele derartiger Schutzziele: a) Transparenz (Information der Betroffenen über Verwendung ihrer Daten beim Training von KI-Modellen; Prüfbarkeit im Sinne der Rechenschaftspflicht), b) Verlässlichkeit (Schutz vor absichtlicher Manipulation; Umgang mit Halluzinationen bei Sprachmodellen) und c) Fairness (Verhinderung unbeabsichtigter Diskriminierung oder Ungleichbehandlung durch die KI). Vertrauenswürdige KI und Datenschutz gehören damit zusammen.

lda.bayern.de/ki04

05 Halluzinationen: Der künstliche Geist bricht manchmal aus

KI auf Basis von neuronalen Netzen kann komplexe Aufgaben lösen, bringt aber zwangsläufig eine gewisse Fehlerhaftigkeit mit sich. Da auch Menschen Fehler machen, kann dies tolerierbar sein, sofern mit möglichen KI-Falschausgaben umgegangen werden kann. Bei großen Sprachmodellen wie ChatGPT tritt diese Fehlereigenschaft allerdings mit einer sehr guten Ausdrucksweise auf. Die KI verfängt sich manchmal in einem „wilden Durcheinander" aus Faktenwissen und Falschaussagen. Diese sporadischen „Halluzinationen" gehören zu großen Sprachmodellen aufgrund ihres Designs dazu und müssen bei einem datenschutzkonformen Einsatz mit berücksichtigt werden.

lda.bayern.de/ki05

06 KI und Mensch: Mitarbeiter für den Einsatz von KI schulen

Da gerade bei erhöhten Risiken ein Mensch die endgültige Kontrolle behalten muss, ist ein vollautomatischer Einsatz von KI in vielen Szenarien nicht realisierbar. Die Mitarbeiter eines Unternehmens sind demnach in Bezug auf die eigene KI zu schulen. Dazu muss der Zweck der KI geregelt und über Fehlerpotentiale informiert werden sowie festgelegt werden, wie mit Ergebnissen der KI umzugehen ist. Insbesondere ist zu schulen, welche (personenbezogene) Daten überhaupt in eine KI eingegeben werden dürfen. Betriebliche Datenschutzbeauftragte können bei diesen Fragestellungen für die Mitarbeiterschulung kompetent mit Rat und Tat zur Seite stehen.

lda.bayern.de/ki06