prompt/

News, Tipps und Debatten zu rechtlichen Fragen rund um generative KI

Mai 2025

Liebe Leser*innen,
Datenschutz gehört für viele bereits zum Alltag. Sei es in regelmäßigen Schulungen der *Datenschutz-Beauftragten* im Unternehmen, in der Hochschule oder in der Behörde. Oder weil man *Datenschutzerklärungen* bei Online-Buchungen oder ärztlichen Behandlungen wortwörtlich abhakt. Datenschutz spielt aber auch beim Einsatz und der Nutzung von generativer Künstlicher Intelligenz eine wichtige Rolle. Denn personenbezogene und sensible Daten können in Datensätzen enthalten sein, die für Trainings von KI-Modellen, das Fine-Tuning von KI-Systemen oder beim Einsatz von KI-Diensten genutzt werden.
Hierbei ist einerseits zu beachten, ob diese Nutzungen erlaubt wurden. Andererseits steht in der Diskussion, wie sich der Schutz solcher Daten in den unterschiedlichen Verarbeitungsschritten bei KI-Systemen wirksam durchsetzen lässt:
Greifen hier die Vorgaben der europäischen KI-Verordnung (KI-VO)? Wenn ja, an welcher Stelle und wer muss sie umsetzen? Oder ist die KI-VO womöglich weit weniger maßgeblich für den Schutz personenbezogener und sensibler Daten, als vielmehr die europäische Datenschutz-Grundverordnung (DSGVO)?
Ausgehend von diesen Fragen beleuchten wir in dieser Ausgabe den aktuellen Stand der Debatte. Zudem berichten Datenschutzbeauftragte von ihrem Praxisalltag bezüglich Beratungen zur Nutzung von KI-Systemen.

Wir wünschen Ihnen viel Freude und Erkenntnisgewinne beim Lesen.
Und wenn Ihnen unser Newsletter **prompt/** gefällt, sagen Sie's gerne weiter – Dankeschön :-)

prompt/ empfehlen

Wenn Sie den **prompt/**-Newsletter regelmäßig bekommen möchten, können Sie sich über diesen Button anmelden:

prompt/ bestellen

Ebenso freuen wir uns über **Themenvorschläge, Fragen oder Erfahrungen aus Ihrem beruflichen oder persönlichen Alltag mit generativer KI.**
Schreiben Sie uns eine E-Mail an prompt@irights-lab.de

Auf bald und mit besten Grüßen,
Ihr **prompt/**-Team

/Inhalt

Monatsthema: Generative KI-Systeme und Datenschutz

- Datenschutz geht weiter | Sticht die DSGVO die KI-VO?
- Transparenz über KI-Trainingsdaten – dank effektivem Datenschutz?
- Aufklärung und Beratung zur Nutzung generativer KI | Interview zum Praxisalltag einer Datenschutzaufsichtsbehörde
- Hintergrund | Information Extraction Attacks

- Weiterlesen | Orientierungshilfe der Datenschutzaufsichtsbehörden | Stellungnahme European Data Protection Board | Bericht der EU-Urheberrechtsbehörde | Berichte der US-Urheberrechtsbehörde
- Über uns | Impressum

/Monatsthema

Sticht die DSGVO die KI-VO?

Die Regelungen zum Datenschutz gelten auch für die Nutzung von KI-Systemen – und betreffen weit mehr Bereiche und Akteur*innen als die Vorgaben der KI-Verordnung

Personenbezogene Daten an Dienstleister und Hersteller von Apps weiterzugeben ist alltäglich und den allermeisten bewusst: Wer sich von einer Navigationsapp zum Ziel leiten lässt, erlaubt oft die Übertragung seiner Standortdaten an den Betreiber; wer das Smart Home-System auffordert, eine Playlist zu starten, übergibt Stimminformationen an die Hersteller; wer Soziale Netzwerke nutzt, erlaubt den Anbietern in der Regel, geteilte Inhalte und das eigene Nutzungsverhalten zu analysieren, um personalisierte Inhalte vorschlagen zu können.

Was aber, wenn diese Daten ohne Zustimmung zum Training von Sprachmodellen genutzt werden? So hat der Datengigant Meta erst vor wenigen Monaten angekündigt, die eigenen KI-Sprachmodelle künftig mit Texten, Bildern, Filmen und weiteren Inhalten der Nutzer*innen seiner Anwendungen Facebook oder Instagram zu optimieren. Ähnlich ist die Online-Plattform X vorgegangen. Bei Facebook lässt sich diese Nutzung nur verhindern, indem man ausdrücklich Widerspruch einlegt. Doch ist das überhaupt rechtens? Was steht zu solchen Datennutzungen in der EU-KI-Verordnung (KI-VO)? Oder greifen in solchen Fällen die Regelungen der Datenschutz-Grundverordnung (DSGVO)?

Die DSGVO nimmt nicht nur KI-Anbieter in den Blick

Die KI-VO nimmt vor allem die Anbieter (*provider*) von KI-Systemen in die Pflicht. Die DSGVO hingegen will *jede* rechtswidrige Verarbeitung personenbezogener Daten verhindern – egal an welcher Stelle der KI-Nutzung sie erfolgt. Immer dann, wenn eine Person dafür verantwortlich ist, dass personenbezogene Daten verarbeitet werden, muss diese Person für die Einhaltung der datenschutzrechtlichen Vorschriften sorgen.

Diese Pflicht betrifft also nicht nur die KI-Anbieter, sondern auch mögliche spätere KI-Betreiber*innen (*deployer*). Die DSGVO orientiert sich dabei an konkreten Verarbeitungsschritten entlang der KI-Wertschöpfungskette: vom Training über die Optimierung bis hin zum Output generativer KI-Systeme. Anders als der Begriff „Kette“ vermuten lässt, sind die unterschiedlichen datenschutzrechtlich verantwortlichen Personen und Stellen allerdings nicht aneinander gekoppelt. Vielmehr ist jeder und jede – unabhängig von den Aktivitäten der anderen – für die Einhaltung datenschutzrechtlicher Bestimmungen voll verantwortlich:

- Am Anfang stehen jene Stellen, die Trainingsdaten für das spätere KI-System erheben, also Inhalte auffinden und auflisten, wie Texte, Bilder, Filme, Musik- und Sprachwerke und so weiter. Sind darunter personenbezogene Daten, handelt es sich um eine datenschutzrelevante Verarbeitung. Das Sammeln, Generieren, Strukturieren und Aufbereiten kann dabei sehr unterschiedlich organisiert sein. Manche erheben Trainingsdaten in eigener Verantwortung, andere lassen sie durch auftragsverarbeitende Dienstleister*innen erheben. Doch unabhängig davon, ob es um *Open Data* und *Open Source* geht oder aufbereitete Datensätze kommerziell auf dem Markt angeboten werden – stets sind die Ausführenden datenschutzrechtlich verantwortlich.

- Auch im nächsten Feld – beim Training und Fine Tuning von KI-Systemen – können schutzrelevante, personenbezogene Daten verarbeitet werden. Ist dies der Fall, gilt es als eigener Verarbeitungsschritt, bei dem entsprechende Schutzmaßnahmen zu treffen sind.

- Auch solche Unternehmen und Stellen, die fertig entwickelte KI-Systeme

erwerben und für eigene Zwecke nutzen wollen, können für den Datenschutz verantwortlich sein. Beispielsweise Dienstleistungsfirmen oder Verwaltungen. Sofern sie ein KI-System nutzen und dort Informationen eingeben (*Input*) eingeben, die personenbezogene Daten enthalten, sind sie verantwortlich dafür, dabei den Datenschutz zu beachten. Ebenso in der datenschutzrechtlichen Verantwortung sind sie dafür, wie sie mit den Ergebnissen umgehen, die ein KI-System liefert (*Output*). Etwa, wenn es in KI-generierten Texten um personenbezogene Bewertungen, Angebote oder Beschreibungen gehen sollte.

Ein Beispiel: Ein Kunde verlangt beim Unternehmen „U-GmbH“ Auskunft darüber, ob seine private Anschrift durch das dort eingesetzte KI-System verarbeitet wird. Das Unternehmen darf nicht darauf verweisen, dass das KI-System von einem externen Dienstleister finegetuned wurde, der deshalb für den Datenschutz in die Pflicht zu nehmen ist. Stattdessen muss die U-GmbH in der Lage sein, dem Kunden eine richtige und vollständige Auskunft über die von ihr verarbeiteten, personenbezogenen Daten zu erteilen. Gelingt dies nicht, so bestehen womöglich Schadenersatzansprüche. Zudem könnten auch aufsichtsrechtliche Bußgelder verhängt werden.

Fazit

Mit seinem Fokus auf einzelne Verarbeitungsschritte geht das Datenschutzrecht sehr kleinteilig vor. Womöglich erweist es sich gerade deshalb als ausschlaggebend dafür, welche KI-Systeme in welcher Weise in der Praxis genutzt werden. Einerseits könnte es Hersteller und Dienstleister dahingehend beeinflussen, auf die Entwicklung und Konfektionierung datenschutzkonformer und transparenter Produkte zu setzen. Andererseits – so fürchten Gegenstimmen bereits – , könnten sich Anbieter von leistungsstarken und wirkmächtigen KI-Systemen aufgrund dieser datenschutzrechtlichen Anforderungen schlicht vom europäischen Markt zurückziehen.

Transparenz über KI-Trainingsdaten – dank effektivem Datenschutz?

In Trainingsdaten von Künstlicher Intelligenz können Daten stecken, die rechtlichen Schutz genießen: urheberrechtlich geschützte Texte oder Fotos, markenrechtlich geschützte Logos von Firmen oder Marken – oder eben personenbezogene Daten wie Name, Anschrift und Personalausweisnummer. Doch ob solche Daten tatsächlich in Trainingsdaten enthalten sind, ist keineswegs leicht festzustellen.

Die Anbieter von großen Sprachmodellen und anderen KI-Systemen lassen in der Regel keine Einblicke in die Trainingsphasen ihrer KI-Systeme zu. Sie berufen sich dabei meist darauf, dass es sich bei den Trainingsdaten um wettbewerbsrelevante Geschäftsgeheimnisse handelt. Was aber sind zum Beispiel die Vorschriften der europäischen Datenschutz-Grundverordnung (DSGVO) noch wert, wenn sie an der „Blackbox KI" scheitern? Hört man in die Diskussionen hinein, dann zeigt sich, dass hierzu noch viele Fragen ungeklärt sind.

Informationspflichten gelten in der KI-VO nur für Hochrisiko-KI

Im Zuge des Gesetzgebungsverfahrens zur europäischen KI-Verordnung (KI-VO) forderten Interessenvertretungen, Nichtregierungsorganisationen und Aufsichtsbehörden, dass KI-Anbietern Veröffentlichungspflichten auferlegt werden sollen: Beispielsweise, indem sie ein Transparenzregister anlegen oder umfangreiche Informationen über ihre KI-Systeme bereitstellen müssen. Doch sollte dies generell für alle KI-Systeme gleichermaßen gelten? Schließlich unterteilt die KI-VO die KI-Systeme in mehrere Risiko-Kategorien.

Letztlich einigten sich die EU-Gesetzgeber darauf, dass eine Informationspflicht zu Trainingsdaten – so steht es nun in der KI-VO – lediglich für *hochriskante* KI-Systeme gilt. Beispielsweise solche, die im Schul- oder Personalwesen eingesetzt werden sollen, und hierfür besonders sensible personenbezogene Daten eine Rolle spielen. Die Anbieter von Hochrisiko-KI-Systemen sind demnach verpflichtet, eine allgemeine Beschreibung der Trainingsdaten als Teil der technischen Dokumentation zu erstellen.

Demgegenüber sind für große Sprach- und Bildmodelle, die in der KI-VO als *weniger riskant* eingestuft werden, zwar ebenfalls Transparenzpflichten angelegt. Was diese Pflichten konkret vorgeben, soll jedoch erst in den sogenannten Praxisleitfäden festgelegt werden, die voraussichtlich in den kommenden Wochen veröffentlicht werden (zu KI-Modellen siehe auch unsere Prompt/-Ausgabe April 2025 /Hintergrund).

Für KI-Systeme mit *geringem Risiko* – beispielsweise Chatbots – sieht die KI-Verordnung dagegen überhaupt keine verpflichtenden Informationen zu den genutzten Trainingsdaten vor.

Das heißt: Um datenschutzrechtliche Pflichten durchzusetzen, helfen die Regelungen der KI-Verordnung allenfalls beim Einsatz von Hochrisiko-KI-Systemen. Wer hingegen sonstige KI-Systeme einsetzt und dabei Wert auf einen datenschutzkonformen Umgang legt, bleibt – was die KI-VO betrifft – weitestgehend auf sich allein gestellt.

Datenschutzaufsichtsbehörden melden sich zu Wort

Damit zeigten sich die deutschen Datenschutzaufsichtsbehörden jedoch nicht

zufrieden und wiesen bereits im Mai 2024 in einer gemeinsam erstellten Orientierungshilfe darauf hin, was die geltende Datenschutz-Grundverordnung (DSGVO) zwingend vorgibt: Unternehmen und Organisationen *müssen* auch bei der Nutzung von KI-Systemen darauf achten und gegebenenfalls aktiv einfordern, „dass Ihnen vom Anbieter ausreichend Informationen zur Verfügung gestellt werden, um die Transparenzanforderungen der Artikel 12 ff. DSGVO umsetzen zu können." Dies umfasst vor allem eine Übersicht der verarbeiteten personenbezogenen Daten sowie den Hinweis darauf, wie sich Daten möglicherweise korrigieren oder löschen lassen.

Die DSGVO geht damit also weiter als die KI-Verordnung: Sie schreibt vor, dass auch Unternehmen und Stellen, die KI-Systeme einsetzen wollen (*Betreiber*), in der Verantwortung sind: Sie *müssen* die jeweiligen Anbieter vertraglich dazu verpflichten, sie sowohl angemessen über die verwendeten Trainingsdaten zu informieren, als auch umfassend über die verarbeiteten personenbezogenen Daten aufzuklären. „Umfassend" meint, dass diese Informationen nicht zu allgemein gehalten sein dürfen und sie vollständig sein müssen – anderenfalls müssen die Betreiber auf mehr Informationstiefe bestehen. Sollten die KI-Anbieter im Zuge ihrer Auskünfte behaupten, für das Training ihrer Systeme ausschließlich anonyme Daten verarbeitet zu haben, dürfen sich die Betreiber auch damit nicht zufrieden geben. (Siehe hierzu auch die Stellungnahme des European Data Protection Board, EDPB.) Vielmehr müssen sie die KI-Anbieter dazu verpflichten, ihnen nachzuweisen, mit welchen technischen und organisatorischen Maßnahmen sie die Trainingsdaten vollständig und wirksam anonymisiert haben.

Datenschutzpflichten für Betreiber von KI-Systemen

Das bedeutet, KI-System-Betreiber müssen einigen Aufwand betreiben, um ihren datenschutzrechtlichen Pflichten nachzukommen. Tun sie dies nicht, können sie als diejenigen, die KI-Systeme einsetzen – und damit datenschutzrechtlich voll verantwortlich sind (siehe Artikel weiter oben) – , durchaus Gefahr laufen, selbst gegen den Datenschutz zu verstoßen und mit Bußgeldern sanktioniert zu werden.

Dieser Rolle und Verantwortung können sie aber womöglich gar nicht immer vollständig gerecht werden. Denn die KI-Anbieter dürften wenig Interesse daran haben, von zahllosen Betreibern etliche Anfragen zu Trainingsdaten-Transparenz zu bearbeiten beziehungsweise vertraglich zu verhandeln. Erfahrungsgemäß neigen die großen KI-Unternehmen aufgrund ihrer exponierten Position dazu, die Bedingungen zu diktieren – sprich, es mit Transparenz zu halten, wie sie wollen.

Fazit

Ob die DSGVO beim Einsatz von KI-Systemen tatsächlich den längeren Hebel bietet, um sensible Daten zu schützen, scheint vorerst eine offene Frage zu bleiben. Zumindest die Betreiber von KI-Systemen, die – wie alle anderen Beteiligten – eine datenschutzrechtliche Verantwortung haben, landen quasi in einer Zwickmühle:

Damit sie KI-Systeme ohne Datenschutzprobleme nutzen können, sind sie auf der einen Seite gezwungen, Transparenz über Trainingsdaten von ihren KI-Anbietern zu erhalten. Auf der anderen Seite entziehen sich große KI-Anbieter erfahrungsgemäß gerne diesen Transparenzpflichten. Und solange die Platzhirsche keine echte Konkurrenz von rechtskonformen agierenden Unternehmen bekommen, solange ist wohl auch keine echte Transparenz zu Trainingsdaten zu erwarten.

/Nachfrage

Aufklärung und Beratung zur Nutzung generativer KI gehören bereits zum Praxisalltag einer Datenschutzaufsichtsbehörde

Interview mit Yvonne Herzog und Daniel Maslewski, Mitarbeiter*in beim Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg.

prompt/: Der datenschutzkonforme Einsatz von generativen KI-Systemen spielt für die öffentliche Verwaltung, aber auch für die Zivilgesellschaft und für Unternehmen eine große Rolle. Wie stellt sich das im Praxisalltag einer Datenschutzaufsichtsbehörde bisher dar?

Yvonne Herzog: Wir versuchen hier ganz bewusst, uns auch proaktiv mit der Materie zu beschäftigen: Beispielsweise veröffentlichen wir Handreichungen und Diskussionspapiere, vermitteln Best Practices, halten und leiten Fachvorträge auf KI-Veranstaltungen oder organisieren Schulungen in unserem eigenen Bildungszentrum (BIDIB). Zur Vorbereitung hierfür gibt es regelmäßig interne Fachkreise und Arbeitsgruppen, an denen unsere KI-Fachreferent*innen aus den verschiedenen Abteilungen teilnehmen.

Daniel Maslewski: Unsere Aufgaben als Aufsichtsbehörde sind sehr vielfältig, weshalb uns die Thematik im Praxisalltag an verschiedenen Stellen begegnet. Es kann beispielsweise sein, dass eine betroffene Person eine Beschwerde bei uns einreicht und dabei eine Datenschutzverletzung durch ein Unternehmen rügt, das KI einsetzt. Oder wir haben ganz konkrete Beratungsanfragen von verantwortlichen Unternehmen oder öffentlichen Stellen, die wissen wollen: Was dürfen wir mit KI machen? Wo gibt es beim Einsatz von KI datenschutzrechtliche Probleme? Worauf müssen wir achten? Je nachdem, von welcher Stelle die Anfrage kommt, können das

auch immer wieder sehr spezifische Problemstellungen sein, die sich auf konkrete KI-Systeme und Verarbeitungsprozesse beziehen. Häufig wird uns aber auch die pauschale Fragen gestellt, ob ein System eingesetzt werden darf. Entscheidend ist daher, dass wir uns gezielt mit innovativen Themen wie KI beschäftigen und unsere Expertise weiter ausbauen.

Yvonne Herzog *ist Sachbearbeiterin KI und Verwaltung in Abteilung 2 (Inneres, Videoüberwachung und Verkehr),* ***Daniel Maslewski*** *ist Referent und Beauftragter für Künstliche Intelligenz / KMU- und Start-up-Beratung in Abteilung 4 (Datenschutz in der Privatwirtschaft), jeweils beim Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg.*

Fotos: privat

prompt/: Warum spielt die schon 2018 in Kraft getretene DS-GVO eigentlich für eine neue Technologie, wie generative KI, überhaupt noch eine Rolle?

Daniel Maslewski: Der Grund hierfür liegt in der bewusst technologieneutralen und innovationsoffenen Ausgestaltung der Datenschutz-Grundverordnung (DS-GVO). Die Vorschriften der Verordnung gelten insoweit grundsätzlich auch bei Datenverarbeitungen im Zusammenhang mit innovativen Technologien wie etwa Künstlicher Intelligenz. Insbesondere beim Training oder beim Einsatz von generativer KI werden regelmäßig große Mengen an personenbezogenen Daten verarbeitet. Dabei kann es sich um ganz verschiedene Arten von Informationen handeln. So können große Trainingsdatensätze beispielsweise unterschiedlichste Inhalte aus dem Internet enthalten – beispielsweise aus Wikipedia oder anderen Plattformen –, in denen Meinungen oder Positionen geäußert werden, die sich auf konkrete Personen zurückführen lassen. Solche Informationen stellen personenbezogene Daten dar. Verantwortliche müssen folglich auch beim Einsatz und Training von KI die datenschutzrechtlichen Anforderungen einhalten und sich mit den KI-spezifischen Problemen auseinandersetzen.

prompt/: Manche Behörden und Unternehmen wünschen sich mehr datenschutzrechtliche Absicherung – zum Beispiel durch klare Aussagen, Bewertungen oder Zertifizierungen von KI-Systemen durch die Aufsichtsbehörden. Wie gehen Sie hier vor?

Daniel Maslewski: Die datenschutzrechtliche Zulässigkeit des Einsatzes von Künstlicher Intelligenz hängt stets von den konkreten Umständen der jeweiligen

Datenverarbeitung ab. Als unabhängige Aufsichtsbehörde prüfen wir die entsprechenden Verarbeitungsvorgänge daher stets einzelfallbezogen. Konkrete Empfehlungen oder pauschale Zertifizierungen für einzelne KI-Anwendungen entsprechen insoweit nicht dem Zweck unserer Aufsichtstätigkeit. Gleichzeitig sehen wir es jedoch als unsere Aufgabe an, verantwortliche Stellen bei der rechtlichen Einordnung zu unterstützen. So haben wir ein Diskussionspapier zu den einschlägigen Rechtsgrundlagen erstellt, das einen Überblick über die datenschutzrechtlichen Anforderungen beim Einsatz von KI bietet und als Grundlage für die weitere Auseinandersetzung dienen soll.

Daneben verfolgen wir in unserer Beratungspraxis das Ziel, ein grundlegendes Verständnis für den datenschutzkonformen Umgang mit KI zu fördern und verantwortliche Stellen für datenschutzrechtliche Fragestellungen zu sensibilisieren. Dabei stellen sich regelmäßig zentrale Fragen wie: Was macht das System, das ich einführen will, mit den geschützten Daten? Gibt es für die Verarbeitung personenbezogener Daten eine einschlägige Rechtsgrundlage? Werden die Daten zu einem anderen Zweck verarbeitet? Wie können die Betroffenenrechte bei intransparenten KI-Systemen umgesetzt werden? Werden die technischen und organisatorischen Maßnahmen eingehalten und entsprechen diese dem Stand der Technik? Wie sieht es mit regelmäßigen Updates aus? Wohin werden die Daten übermittelt? Werden abgeschottete Systeme verwendet, bei denen der KI-Anbieter nicht dauerhaft auf eure Datensätze zugreifen kann?

Yvonne Herzog: Wichtig ist auch, dass die von der DSGVO vorgesehene Rollenverteilung klar wird: Arbeitet ein Unternehmen oder eine öffentliche Einrichtung mit personenbezogenen Daten, hat das Unternehmen oder die Einrichtung die Pflicht und Verantwortung, diese zu schützen. Der größte Fehler, den man machen kann, ist, sich nicht aktiv mit den Fragen auseinanderzusetzen, weil mir zum Beispiel mein KI-Anbieter sagt: Es passt schon alles!

/Hintergrund

Information Extraction Attacks

Unter dem Begriff Information Extraction Attacks (auch: Model Inversion Attacks) verstehen Fachleute eine Methode, um herauszubekommen, ob in einem großen, vielfältigen Datenbestand ganz bestimmte Daten enthalten sind. Sie lässt sich auch auf KI-Systeme anwenden. Vereinfacht gesagt, sollen bestimmte Prompts dazu dienen, den KI-Systemen präzise und umfangreiche Informationen über die darin verwendeten Trainingsdaten zu entlocken.

Tatsächlich ist diese Methode in der Wissenschaft und bei Aufsichtsstellen, wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI), bereits gut bekannt. Und sie kann sogar – je nach KI-System – auch von ungeübten Nutzer*innen genutzt werden: Die europäische Datenschutzorganisation None of Your Business (NOYB) hatte bereits im April 2024 bei der Österreichischen Datenschutzbehörde eine Beschwerde gegen den KI-Anbieter OpenAI eingereicht, weil dessen Chatbot Chat GPT falsche personenbezogene Daten zu einer bestimmten Person ausgegeben hatte. Laut NOYB könnte dies „von jedem, der ein ChatGPT-Konto hat, leicht überprüft werden."

Des einen Freud ist des anderen Leid

Wenn KI-Anbieter verhindern wollen, dass ihre KI-Systeme durch Information Extraction Attacks personenbezogene Daten ausgeben, müssen sie mittels technischer Hindernisse für eine datenschutzrechtlich effektive und wirksame Anonymisierung sorgen. Mehr noch: Sie müssten womöglich sogar Information Exctraction Attacks gegen die eigenen Systeme durchführen lassen, um eventuelle Schwachstellen zu identifizieren und zu beheben.

Für Urheber*innen und Rechteinhaber*innen hingegen könnte das zum Problem werden. Sie nutzen Information Extraction Attacks, um herauszufinden, ob KI-Systeme Inhalte erzeugen können, die sehr nah an geschützten Originalwerken sind und damit womöglich Urheberrechte verletzen. Darauf beruft sich zum Beispiel die Verwertungsgesellschaft GEMA in ihrer Klage gegen den Musik-KI-Anbieter Suno (siehe **prompt/**-März-Ausgabe). Würden die oben beschriebenen Anonymisierungsmaßnahmen greifen, ließe sich womöglich nicht mehr nachweisen, dass in den Trainingsdaten urheberrechtlich geschützte Werke enthalten sind. Im Ergebnis könnten also datenschutzkonforme, „anonymisierte KI-Systeme" dazu beitragen, Urheber*innen in der Durchsetzung ihrer Rechte zu behindern.

/Weiterlesen

Artikel und Quellen zu generativer KI

Bereits im Mai 2024 veröffentlichten die Datenschutzaufsichtsbehörden des Bundes und der Länder eine gemeinsam erstellte Orientierungshilfe zu KI und Datenschutz.

Stellungnahme des Europäische Datenschutzausschuss (EDSA) zu Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen („Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the

context of AI models.“) Der Europäische Datenschutzausschuss (EDSA) ist ein unabhängiges europäisches Gremium und Dachorganisation der nationalen Datenschutzbehörden (Nationale Aufsichtsbehörden) der Länder des Europäischen Wirtschaftsraums sowie der Europäischen Datenschutzbeauftragten (EDPS).

In einer umfangreichen Handreichung geht das Bundesamt für Sicherheit in der Informationstechnik (BIS) auf die Chancen und Risiken für Industrie und Behörden bei der Nutzung von Modellen mit generativer KI ein.

In der Handreichung des Paritätischen Gesamtverbands zu Rechtsfragen beim Einsatz von generativer KI in gemeinnützigen Organisationen geht es auch um die wesentlichen Fragen zum Datenschutz (ab Seite 18).

Die EU-Urheberrechtsbehörde, EUIPO, beschäftigt sich in einem ausführlichen Bericht mit der„Entwicklung generativer künstlicher Intelligenz aus der Perspektive des Urheberrechts“.

Auch die US-Amerikanische Urheberrechtsbehörde hat sich in bisher drei umfangreichen Reports mit Aspekten von Urheberrecht und Künstlicher Intelligenz auseinandergesetzt: „Copyright and Artificial Intelligence“. Seit kurzem liegt eine Vorveröffentlichung des dritten Berichts zu urheberrechtlichen Fragen bei KI-Trainings vor: „Generative AI Training“.

Die freie Enzyklopädie Wikipedia setzt auf KI. Wie das Portal Golem berichtet, will die Wikimedia Foundation ihren Editoren und Moderatoren ermöglichen, in der Wikipedia KI-gestützte Werkzeuge einzusetzen, wobei die menschliche Qualitätssicherung weiterhin Priorität haben soll.

/Über uns | Impressum

Diesen Newsletter erstellen und produzieren wir, das iRights.Lab, im Rahmen des Forschungsprojekts *Generative KI – Innovation und Recht in Arbeitsprozessen (GenKI-IR)*, gefördert vom Bundesministerium für Bildung und Forschung (BMBF).

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Das Projekt hat zum Ziel, rechtliche und gesellschaftliche Rahmen zu beschreiben, mit denen Anwendungen

generativer KI unterschiedliche Arbeitsprozesse sinnvoll unterstützen können.

Texte: Matthieu Binder, Henry Steinhau
Redaktion: Henry Steinhau (verantwortlich), Merlin Münch
Mitarbeit und Lektorat: Solvejg Gunkel, Ella Jordan
Rechtehinweis: Alle Texte und Bilder stehen unter der offenen Lizenz CC-BY 4.0, außer die Porträts Yvonne Herzog und Daniel Maslewski (jeweils privat).

iRights.Lab GmbH

www.irights-lab.de

Oranienstr. 185

10999 Berlin

prompt@irights-lab.de

Tel: +49 30 40 36 77 230

Fax: +49 30 40 36 77 260

Steuernr. 37/359/5262 | USt‍ID DE311181302

Registergericht:

Amtsgericht Charlottenburg Nr. HRB 185640 B

Geschäftsführer*innen:

Philipp Otto, Dr. Wiebke Glässer