Rechtsgrundlagen für den Einsatz von Künstlicher Intelligenz in der Verwaltung

1. Rechtliche Rahmenbedingungen beim Einsatz von KI

Rund um das Thema Künstliche Intelligenz (KI) und deren Nutzung im Dienstbetrieb sind grundsätzlich verschiedene rechtliche Aspekte zu beachten, die in diesem Dokument behandelt werden.

2. Entwurf einer europäischen KI-Verordnung

2.1. Grundlegendes und aktueller Stand

Die geplante KI-Verordnung der Europäischen Union (EU) zielt darauf ab, den Einsatz von Künstlicher Intelligenz sicherer und ethischer zu gestalten. Sie legt Regeln und Anforderungen fest, die vordringlich den Anbieter in den Blick nehmen. Daneben gelten weitere Vorgaben auch für sog. Produkthersteller, Einführer, Händler, Betreiber und Nutzer. Das Hauptanliegen des europäischen Gesetzgebers ist es, Bürger vor potenziellen Risiken und Diskriminierung im Zusammenhang mit KI-Systemen zu schützen, während gleichzeitig Innovation und Wettbewerbsfähigkeit gefördert werden sollen. Die Verordnung folgt dabei einem **risikobasierten Ansatz**, wobei eine Einstufung in verschiedene Risikoklassen erfolgt. Während sog. Verbotene Praktiken in KI-Systemen stets unzulässig sind, gelten z. B. für sog. Hochrisiko-KI-Systeme strenge Vorgaben. Die Einstufung hängt insbesondere von der Zweckbestimmung und den konkreten Anwendungsbereichen des jeweiligen KI-Systems ab. Durch die künftige unionsweite Regulierung soll Vertrauen und ein konsequent hoher Schutz von Sicherheit und Grundrechten gewährleistet werden („**AI Made in Europe**“).

Die Kommission legte einen Entwurf für eine KI-Verordnung bereits am 21. April 2021 vor[1]. Der Rat veröffentlichte seine in einigen Punkten abgeschwächte Position zum Legislativvorschlag am 6. Dezember 2022. Das Europäische Parlament verabschiedete seine finale Position am 14. Juni 2023. Die Abstimmungen zwischen Parlament, Rat und Kommission (sog. Trilog-Verhandlungen) endeten mit einer Einigung am 8. Dezember 2023. Am 13.02.2024 haben die Ausschüsse für

[1] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM/2021/206 final).

Binnenmarkt und bürgerliche Freiheiten (IMCO, LIBE) des Europäischen Parlaments den Kompromisstext gebilligt, der zwischenzeitlich in deutscher sowie konsolidierter Fassung vorliegt[2]. Nachdem das Europäische Parlament am 13. März 2024 mehrheitlich für das Gesetz gestimmt hat, steht noch die endgültige Billigung durch den Rat aus. Anschließend besteht gem. Art. 113 KI-VO grundsätzlich eine Übergangsfrist von 24 Monaten.

Nach Art. 3 Nr. 1 KI-VO ist das der Verordnung unterfallende „**KI-System**" definiert als „maschinengestütztes System, das für einen in wechselndem Maße autonomen Betrieb ausgelegt sind [sic!], das nach seiner Einführung anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ergebnisse wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen hervorgebracht werden, die physische oder virtuelle Umgebungen beeinflussen können".

Für sämtliche (im Nachfolgenden im Einzelnen dargestellte) Risikoklassen des KI-Systems gilt gemäß Art. 4 KI-VO die **Pflicht für Anbieter und Betreiber von KI-Systemen zur Schaffung von „AI literacy"** mit einer **Übergangsfrist** von nur 6 Monaten (Art. 113 lit. a KI-VO). Der Begriff „AI literacy" („KI-Kompetenz") bezieht sich auf Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden (vgl. Art. 3 Nr. 56 KI-VO). In Art. 4 KI-VO ist geregelt, dass die Anbieter und Betreiber von KI-Systemen Maßnahmen ergreifen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind.

Die nachfolgende Darstellung basiert auf dem Dokument A9-0188/808 ("Abänderungen des Europäischen Parlaments zum Vorschlag der Kommission") des Europäischen Parlaments vom 6. März 2024 in der deutschen übersetzten Sprachfassung, abrufbar unter: https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_DE.pdf.
Änderungen, die sich infolge der finalen deutschen Sprachfassung ergeben, bleiben vorbehalten.

2 https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_DE.pdf. Im Folgenden zitiert als: KI-VO.

2.2. Risikoklassen und Folgen der jeweiligen Einstufung

Die vier **verschiedenen Risikoklassen** samt Einstufung der sogenannten „KI-Modelle mit allgemeinem Verwendungszweck“ der KI-Verordnung sind im Überblick:

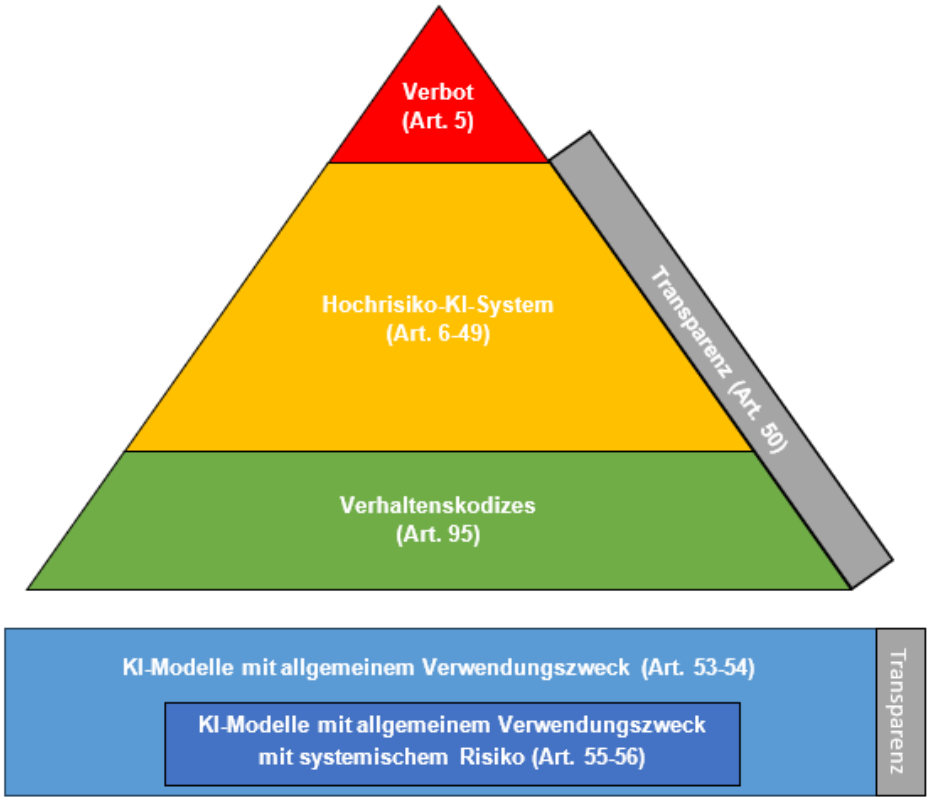


Abbildung 1: Aktualisierte Grafik in Anlehnung an Bomhard/Siglmüller, RDi 2024, 45, 46.

1. **Unzulässige KI: verbotene Praktiken**

   Art. 5 Abs. 1 KI-VO enthält eine Liste an Vorgaben zu **verbotenen** KI-Systemen. Diese werden als unvereinbar mit den Grundrechten der EU angesehen. Hierbei geht es etwa um manipulative oder täuschende Techniken zur unterschwelligen Beeinflussung von Personen, um Social Scoring (d.h. Bewertung von Personen anhand von persönlichen Merkmalen wie Geschlecht, Religion oder politischer Überzeugung) oder um Datenbanken zur Gesichtserkennung durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen. Die Kommission führt als Beispiel für ein verbotenes KI-

System ebenso ein Spielzeug mit Sprachassistent, das Kinder zu riskantem Verhalten verleitet, auf.[3]

Wird gegen das Verbot von Praktiken im Bereich der KI aus Art. 5 KI-VO verstoßen, sieht Art. 99 Abs. 3 KI-VO Geldbußen von bis zu **35 Millionen Euro** oder **7 % des gesamten weltweiten Jahresumsatzes eines Unternehmens im vorangegangenen Geschäftsjahr** vor, wobei von den beiden dargestellten Alternativen der höhere Betrag maßgeblich ist.

2. Hochrisiko-KI

Ein KI-System kann nach Art. 6 Abs. 1 oder Abs. 2 i. V. m. Anhang III KI-VO als sog. **Hochrisiko-KI-System** gelten. In Anhang III werden folgende Bereiche genannt, die Hochrisiko-KI bedeuten können, sofern das KI-System zugleich - vgl. die Ausnahme in Art. 6 Abs. 3 KI-VO - ein erhebliches Risiko für die Gesundheit, die Sicherheit oder die Grundrechte von natürlichen Personen darstellt:[4]

- **Biometrische Fernidentifizierung** und auf Biometrie beruhende Systeme, durch die Rückschlüsse auf sensitive oder geschützte Attribute gezogen werden, einschließlich Systeme zur Emotionserkennung
- Verwaltung und Betrieb **kritischer Infrastrukturen** (im Straßenverkehr oder bei der Wasser-, Gas-, Wärme- und Stromversorgung; ebenso ist die digitale kritische Infrastruktur erfasst), wobei die KI-Systeme bestimmungsgemäß als Sicherheitskomponenten verwendet werden
- Allgemeine und berufliche **Bildung**, wenn der Zugang einer Person zur Bildung und zum Berufsleben beeinträchtigt werden könnte (z. B. Bewertung von Prüfungen oder bei der Prüfungsaufsicht)
- **Beschäftigung**, **Personalmanagement** und Zugang zur Selbstständigkeit (z. B. Software zur Auswertung von Lebensläufen für Einstellungsverfahren)
- Zugänglichkeit und Inanspruchnahme **grundlegender privater und grundlegender öffentlicher Dienste** und Leistungen (z. B. Bewertung der Kreditwürdigkeit, wodurch Bürgern Darlehen verwehrt werden können oder zur Entscheidung über die Möglichkeit des Abschlusses einer Kranken- oder Lebensversicherung)
- **Strafverfolgung** (z. B. zur Entscheidung über eine Strafaussetzung zur Bewährung, Einsatz von Lügendetektoren)

---

[3] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_de.

[4] Vgl. auch zum Nachfolgenden https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_de.

- **Migration, Asyl und Grenzkontrolle** (z. B. Unterstützung der Behörden bei der Prüfung von Anträgen auf Asyl, Visum und Aufenthaltstitel)
- **Rechtspflege** und **demokratische Prozesse** (z. B. Anwendung von Rechtsvorschriften auf konkrete Sachverhalte durch Gerichte, KI-Systeme im Zusammenhang mit Wahlen)

Die Klassifizierung als Hochrisiko-KI-System ist **mit erheblichen Anforderungen** an das KI-System **verbunden** (Art. 8-15 KI-VO). Zum Beispiel muss ein Risikomanagement-System vorgehalten werden und für ein Datentraining müssen die Trainings-, Validierungs- und Testdaten bestimmte Anforderungen erfüllen. Neben weiteren Beteiligten unterliegen die **Anbieter und Betreiber** von Hochrisiko-KI-Systemen einer Vielzahl von Pflichten (Art. 16-27 KI-VO). Zum Nachweis, dass die Anforderungen erfüllt werden, muss der Anbieter eine **Konformitätsbewertung** für sein KI-System einholen (Art. 43 KI-VO). Die Konformitätsbewertungsstellen müssen in den Mitgliedstaaten notifiziert werden (Art. 31 KI-VO). Sowohl **vor Inverkehrbringen** als auch während des **gesamten Lebenszyklus** des KI-Systems müssen entsprechende Anforderungen erfüllt sein.

Die Europäische Kommission fasst die nach der künftigen Regulierung **notwendigen Schritte für Anbieter von Hochrisiko-KI-Systemen** wie folgt grafisch zusammen:

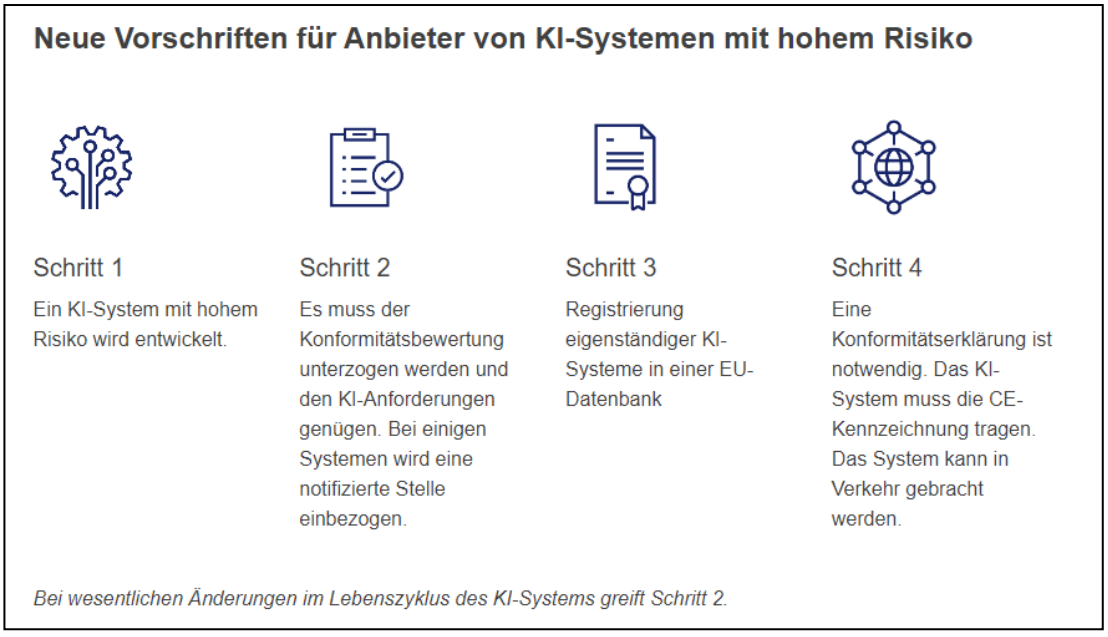


Abbildung 2: Europäische Kommission, Quelle: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_de

2.3. Regulierung von „KI-Modellen mit allgemeinem Verwendungszweck“

Einen wesentlichen Streitpunkt, der beinahe ein Scheitern der Trilog-Verhandlungen verursacht hätte, bildet die Regulierung von KI-Systemen, die keinen spezifischen Zweck verfolgen, sondern allgemein zur Text-, Bild- und Videogenerierung, Bild- oder Spracherkennung etc. eingesetzt werden können. Die KI-VO spricht hier von sogenannten „KI-Modellen mit allgemeinem Verwendungszweck“, für die in Art. 51 bis Art. 56 KI-VO bestimmte Regelungen vorgesehen sind. Art. 51 KI-VO definiert für die „KI-Modelle mit allgemeinem Verwendungszweck“ wiederum zwei Risikoklassen mit unterschiedlichen Pflichtenkatalogen: „einfache“ KI-Modelle und solche mit „systemischen Risiko“.[5]

„Einfache“ Modelle müssen entsprechenden Transparenzanforderungen genügen. Dazu gehören nach Art. 53 KI-VO die Erstellung einer technischen Dokumentation, die Einhaltung des EU-Urheberrechts und die Bereitstellung detaillierter Zusammenfassungen über die für das Training verwendeten Inhalte.

Für Modelle „mit systemischen Risiko“ gelten gem. Art. 55 KI-VO strengere Anforderungen. Wenn diese Modelle bestimmte Kriterien erfüllen, müssen sie Modellevaluierungen durchführen, systemische Risiken bewerten und abschwächen, Gegentests durchführen, der EU-Kommission über schwerwiegende Vorfälle berichten und Cybersicherheit gewährleisten. Bis zur Veröffentlichung harmonisierter EU-Standards, vgl. Art. 40 KI-VO, sollen sie auf Verhaltenskodizes (vgl. Art. 56 KI-VO) zurückgreifen können, um die Pflichten der KI-Verordnung einzuhalten.

[5] Hierzu grundlegend: https://www.europarl.europa.eu/news/de/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.

3. Urheberrecht

Die Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe des Gesetzes über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz – UrhG). Das Urheberrecht besteht per se mit der Erstellung eines Werkes im Sinne des UrhG. In diesem Kontext ergeben sich beim Einsatz von KI verschiedene Fragestellungen zum Urheberrecht, die nachfolgend beleuchtet werden.

3.1. Urheberrecht – Verwendung urheberrechtlich geschützter Daten zum Training einer KI

Trainingsdaten einer KI werden in der Regel verwendet, um aus diesen zu „lernen“. Das Urheberrecht findet Anwendung auf die Trainingsdaten, sobald die Daten – wenn auch nur übergangsweise – vervielfältigt werden. Dies wird in der Praxis unumgänglich sein. Grundsätzlich bedarf es zur Verwendung urheberrechtlich geschützter Werke wie Texte oder Bilder zur Verwendung als Trainingsdaten daher der Erlaubnis des Urhebers oder einer gesetzlichen Erlaubnis.

§ 44b UrhG ermöglicht jedoch ein grundsätzlich lizenzfreies Training einer KI mit Hilfe urheberrechtlich geschützter Werke, sofern Text oder Data Mining betrieben und dabei folgende Voraussetzungen gegeben sind. § 44b UrhG definiert Text und Data Mining als automatisierte Analyse von einzelnen oder mehreren digitalen oder digitalisierten Werken, um daraus Informationen insbesondere über Muster, Trends und Korrelationen zu gewinnen.

- Zulässig sind Vervielfältigungen von rechtmäßig zugänglichen Werken für das Text und Data Mining.
- Vervielfältigungen sind zu löschen, wenn sie für das Text und Data Mining nicht mehr erforderlich sind.
- Text und Data Mining ist jedoch nur zulässig, wenn der Rechtsinhaber sich diese Nutzung nicht vorbehalten hat. Ein solcher Nutzungsvorbehalt bei online zugänglichen Werken ist nur dann wirksam, wenn er in maschinenlesbarer Form erfolgt.

In der Praxis wird sich somit grundsätzlich die Frage stellen, ob die für die KI zum Training vorgesehenen Daten rechtmäßig zugänglich sind und nicht einem Nutzungsvorbehalt unterliegen.

Zukünftige rechtliche Entwicklungen hinsichtlich des Machine Learnings für KI werden fortlaufend zu berücksichtigen sein.

3.2. Urheberrechtliche Aspekte bei der Nutzung eines KI-Systems

Persönliche geistige Schöpfungen im Sinne des Urheberrechtsgesetzes (§ 2 Abs. 2 UrhG) genießen den besonderen Schutz unserer Rechtsordnung; gleiches gilt für verwandte Schutzwerke wie insbesondere Lichtbildwerke (§ 72 UrhG). In beiden Fällen wird der gesetzliche Schutz jedoch wiederum durch zwingende Ausnahmetatbestände eingeschränkt. Beim Einsatz von KI ist daher Vorsicht im Hinblick auf den Urheberrechtsschutz angebracht, wobei aber keinesfalls jedes bestehende Urheberrecht dem Einsatz von KI in der öffentlichen Verwaltung entgegensteht.

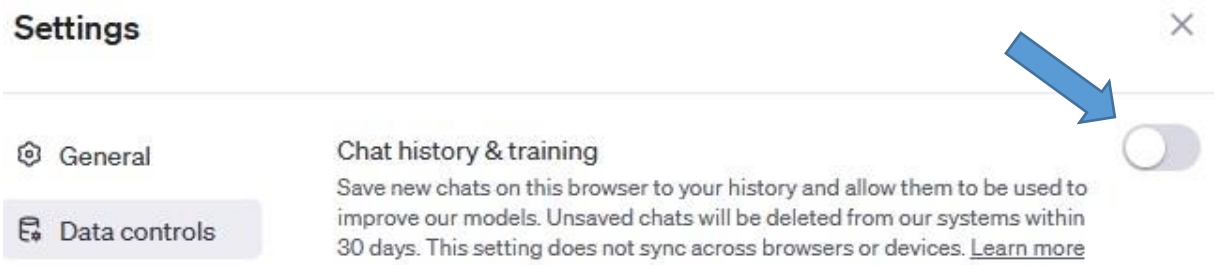
3.2.1. Eingabe urheberrechtlich geschützter Werke in den Prompt der KI

Eingaben urheberrechtlich geschützter Werke in den Prompt einer KI sind nicht von vornherein unzulässig. Dies betrifft z. B. von Dritten verfasste Texte, die von einem Sprachmodell analysiert oder zusammengefasst werden sollen oder Bildwerke, die als Eingabe in eine generative KI-Anwendung verwendet werden sollen.

§ 44a UrhG erlaubt sog. „vorübergehende Vervielfältigungshandlungen“, die nur flüchtig oder begleitend sind und dabei einen integralen und wesentlichen Teil des technischen Verfahrens darstellen, welches dem Betrieb des KI-Systems dient. Dabei ist erforderlich, dass alleiniger Zweck der vorübergehenden Vervielfältigungshandlungen ist, dass eine Übertragung in einem Netz zwischen Dritten durch einen Vermittler (§ 44a Nr. 1 UrhG) oder eine rechtmäßige Nutzung (§ 44a Nr. 2 UrhG) eines Werkes oder sonstigen Schutzgegenstands ermöglicht wird, und die vorübergehenden Vervielfältigungshandlungen keine eigenständige wirtschaftliche Bedeutung haben. Es ist unter Einhaltung dieser Voraussetzungen also grundsätzlich erlaubt, ein (wenn auch urheberrechtlich geschütztes) Werk in den Prompt zu kopieren, um damit einen von der KI generierten Output zu erschaffen. Der Wortlaut des § 44a UrhG setzt allerdings eine „rechtmäßige Nutzung“ des Werkes voraus. Das ist der Fall, wenn die in den Prompt eingegebenen Daten dem Nutzer rechtmäßig zur Verfügung stehen, wenn sie also z. B. für jedermann zugänglich im Internet veröffentlicht wurden oder – falls die Daten nur entgeltlich zur Verfügung stehen – vom Nutzer erworben wurden. Ferner darf die Eingabe in den Prompt „keine eigenständige wirtschaftliche Bedeutung“ besitzen. Dieses Tatbestandsmerkmal wäre zum Beispiel problematisch, wenn die generative KI-Anwendung dazu verwendet werden würde, urheberrechtlich geschützte Werke inhaltlich abzuwandeln und in dieser Form kommerziell weiterzuverwenden.

Es ist jedoch darauf hinzuweisen, dass viele öffentlich nutzbare KI-Systeme die in den Prompt eingegebenen Daten über längere Zeit speichern, da die Anbieter die Prompt-Eingaben häufig wiederum zum Training der KI verwenden. Unter diesen Umständen kann zweifelhaft sein, ob der Erlaubnistatbestand der bloß „vorübergehenden Vervielfältigungshandlung“ noch erfüllt ist. Jedoch bieten zahlreiche KI-Systeme wie z. B. ChatGPT die Möglichkeit, in den Systemeinstellungen ein ausdrücklichs Opt-Out gegen die Verwendung der Prompts zu Trainingszwecken zu erklären (s.

die untenstehende Grafik in Bezug auf ChatGPT). Zumindest bei der Eingabe urheberrechtlich geschützter Werke in den Prompt ist von diesem Opt-Out Gebrauch zu machen.



3.2.2. Eigener urheberrechtlicher Schutz des Prompts

Darüber hinaus stellt sich die Frage, ob der Prompt, also die vom Nutzer getätigte Eingabe, selbst urheberrechtlichen Schutz genießt. Das ist in aller Regel zu verneinen, da das Urheberrecht nur „persönliche geistige Schöpfungen“ (§ 2 Abs. 2 UrhG) mit einer gewissen geistigen „Schöpfungshöhe“, nicht aber rein technische Arbeitsanweisungen schützt.

Es ist unter Gesichtspunkten des Urheberrechts also grundsätzlich zulässig, von Dritten erstellte Prompts weiterzuverwenden, solange sie den Charakter einfacher Arbeitsanweisungen haben – wie beispielsweise die Eingabe: „Schreibe eine Rede für einen Politiker, die Chancen und Risiken des Einsatzes von KI in der öffentlichen Verwaltung thematisiert.“

Abweichend davon können Prompts ausnahmsweise urheberrechtlichen Schutz genießen, wenn sie umfangreiche und komplexe Handlungsanweisungen enthalten, die in der Lage sind, die Arbeitsergebnisse des KI-Systems bis ins Detail zu steuern. Solche komplexen Prompts werden häufig von Experten erstellt („Prompt Engineering“) und nur gegen Entgelt zur Verfügung gestellt.

3.2.3. Urheberrechtlicher Schutz des von der KI erzeugten Outputs

Der von einer KI-Anwendung generierte Output – insbesondere Texte oder Bilder, die von Systemen wie Chat-GPT oder DALL-E „erschaffen“ wurden – unterfällt regelmäßig nicht dem Schutz des Urheberrechts. Es fehlt nämlich an dem Merkmal der „persönlichen“ Schöpfung durch eine natürliche Person, die § 2 Abs. 2 UrhG fordert. Auch die Nachahmung eines bestimmten Stils begründet dabei noch nicht allein ein Urheberrecht. Ein KI-generierter Output wird regelmäßig auch nicht unter einem „verwandten Schutzrecht“ im Sinne des UrhG stehen; er stellt etwa keine „Lichtbilder“ nach § 72 UrhG dar, weil er nicht durch fotografische oder vergleichbare Verfahren erzeugt wurde. Zum Teil wird allerdings ein Schutz des KI-generierten Outputs durch die Leistungsschutzrechte für Film- oder Tonträgerhersteller für möglich gehalten, da diese ausschließlich Investitionsschutz bezwecken.

Im Ergebnis begegnet es in den meisten Fällen keinen urheberrechtlichen Bedenken, die Ausgabe der KI zu eigenen Zwecken der öffentlichen Verwaltung zu verwenden. Ausnahmen bestehen jedoch, wenn die KI-Anwendung ein urheberrechtlich geschütztes Werk oder Teile davon kaum oder nur leicht verändert reproduziert hat, sodass die ursprüngliche Urheberschaft noch deutlich erkennbar ist. Das kann insbesondere der Fall sein, wenn der Nutzer die KI-Anwendung nur zur Suche bzw. Wiedergabe bestimmter Werke oder Werkteile genutzt hat. Bekannt sind auch Fälle bildgenerierender KI-Systeme, die reale Künstlerunterschriften kopiert haben. Von der Weiterverwendung, insbesondere der Veröffentlichung eines KI-Outputs ist daher zumindest dann abzusehen, wenn er eindeutige „Plagiate“ enthält.

Obwohl KI-generierte Texte und Bilder, die Dritte ins Internet gestellt haben, prinzipiell nicht unter urheberrechtlichem Schutz stehen, empfiehlt es sich – nebenbei bemerkt – trotzdem nicht, diese zu kopieren und auf Websites des Freistaats zu verwenden. Es kann nämlich selten sicher bestimmt werden, ob solche Inhalte menschlich nachbearbeitet wurden, was unter Umständen wieder zu einem Schutz nach dem UrhG führen kann.

4. Datenschutzrecht

Eine entscheidende Rolle sowohl beim Training als auch beim Einsatz von KI-Anwendungen nimmt das Datenschutzrecht ein. Damit sowohl die Rechte betroffener Personen angemessen geschützt als auch die Nutzung von KI-Anwendungen überhaupt erst ermöglicht werden kann, ist es besonders wichtig, datenschutzrechtliche Bestimmungen von der Planung bis zur Umsetzung in jeder Phase mit zu berücksichtigen. Das umfasst auch die frühzeitige und konstante Einbindung der behördlichen Datenschutzbeauftragten.

4.1. Allgemeines

Die KI-Verordnung trifft im Bereich Datenschutz nur sehr wenige Regelungen, die lediglich Hochrisiko-KI und biometrische Fernidentifizierungssysteme betreffen, und stellt keine Datenverarbeitungsbefugnisse bereit. Die Datenschutzgrundverordnung (DSGVO) soll aber – nach Erwägungsgrund 72 der KI-VO – „unberührt“ bleiben. Auch die DSGVO, die seinerzeit – nach Erwägungsgrund 15 der DSGVO – bewusst technologie-neutral gefasst wurde, enthält keine spezifischen Regelungen für KI-Anwendungen. Das bedeutet, dass die Anforderungen der DSGVO, insbesondere das zwingende Erfordernis einer Rechtsgrundlage für die Datenverarbeitung, immer dann zu beachten sind, wenn personenbezogene Daten verarbeitet werden. Personenbezogene Daten sind gemäß Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Die in der Definition einbezogene Ausweitung des Begriffs auf identifizierbare Personen bedeutet, dass möglicherweise auch Informationen, die auf den ersten Blick nicht als personenbezogenes Datum eingestuft werden, aus dem Sinnzusammenhang und bei Auslegung des Kontextes einen entsprechenden Personenbezug herstellen können (beispielsweise: „das gelbe Haus in der Max-Mustermann-Str.“ – dabei handelt es sich unter Umständen um ein personenbezogenes Datum, wenn in der entsprechenden Straße nur ein gelbes Haus existiert). Personenbezogene Daten können zu unterschiedlichen Zeitpunkten in KI-Anwendungen verarbeitet werden, entweder bereits beim Training oder auch erst bei der späteren Nutzung der KI-Anwendung im Verwaltungsalltag.

4.2. Rechtsgrundlage für KI-Anwendungen

Behörden verarbeiten personenbezogene Daten in der Regel auf Basis der Rechtsgrundlage des Art. 6 Abs. 1 UAbs. 1 Buchstabe e DSGVO, in Verbindung mit einer spezialgesetzlichen oder allgemeinen Datenverarbeitungsbefugnis im Sinne von Art. 6 Abs. 3 DSGVO, das heißt die Verarbeitung muss zur Wahrung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Bedient sich eine Behörde bei ihren Verarbeitungstätigkeiten einer KI-Anwendung zur Erfüllung ihrer Aufgaben, stellt die KI-Anwendung nach der hier vertretenen Auffassung ein sogenanntes Betriebsmittel dar, das den Beschäftigten bei der Erfüllung seiner Aufgabe unterstützt. Eine KI-Anwendung kann – wie andere Betriebsmittel auch – ihrerseits eigene personenbezogene Daten („spezifische Betriebsmitteldaten“) verarbeiten, zum Beispiel IP-Adressen der Nutzer („spezifische Betriebsmitteldaten“). Dies ist bei einer Risikoanalyse zu berücksichtigen. Im Zusammenhang mit dieser Datenverarbeitung muss darauf geachtet werden, dass keine Leistungs- und Verhaltenskontrolle der Nutzer erfolgt. Im Hinblick auf etwaige Beteiligungsrechte der Personalvertretungen wird auf Ziff. 5.1 verwiesen.

4.3. Training von KI-Anwendungen und Rechtsgrundlage

Wie bereits dargestellt, werden KI-Anwendungen überwiegend mittels großer Datensätze trainiert. In diesen Datensätzen ist häufig eine große Menge personenbezogener Daten enthalten[6]. Werden die Inhalte für das Training nicht um die personenbezogenen Daten durch Anonymisierung oder ähnliche Prozesse bereinigt, handelt es sich um eine datenschutzrechtliche Verarbeitung nach Art. 4 Nr. 2 DSGVO, die das Vorliegen einer Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 DSGVO erfordert.[7] Das Training umfasst das Einbringen von Daten als Trainingsdaten, die spätere Validierung und die anschließende Testung der Anwendung.[8]

In der Literatur[9] wird dazu vertreten, zum Training von KI-Anwendungen könne gegebenenfalls Art. 6 Abs. 1 UAbs. 1 Buchstabe a DSGVO, also die Einwilligung, herangezogen werden. Das ist allerdings bei großen Datenmengen voraussichtlich sowohl im Hinblick auf die Identifizierbarkeit und die Anzahl der etwaig betroffenen Personen als auch im Hinblick auf die Widerrufbarkeit der Einwilligung wenig praktikabel[10].Für nichtöffentliche Stellen kommt zudem Art. 6 Abs. 1 UAbs. 1

---

[6] Franke, Datenschutzrechtskonformes Training von KI-Systemen mit öffentlich verfügbaren personenbezogenen Daten, RDi 2023, 565

[7] Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz (Stand: 07. November 2023), S. 7 f.

[8] Hessel/Dillschneider, datenschutzrechtliche Herausforderungen beim Einsatz von Künstlicher Intelligenz, RDi 2023, 458

[9] Franke, Datenschutzrechtskonformes Training von KI-Systemen mit öffentlich verfügbaren personenbezogenen Daten, RDi 2023, 565

[10] Ashkar: Wesentliche Anforderungen der DS-GVO bei Einführung und Betrieb von KI-Anwendungen, ZD 2023, 523

Buchstabe f DSGVO, das berechtigte Interesse, in Betracht. Dieses scheidet allerdings nach Art. 6 Abs. 1 Abs. 2 DSGVO für Behörden aus.

Um an dieser Stelle Rechtssicherheit zu schaffen, sieht der Digitalplan vor, an einer bayerischen Lösung zu arbeiten und eine Rechtsgrundlage zur Datenverarbeitung im Rahmen des Trainings, der Validierung und der Weiterentwicklung von KI-Anwendungen zu schaffen.

4.4. Fine-Tuning einer erworbenen und austrainierten KI-Anwendung und Rechtsgrundlage

Werden sogenannte „ready-to-use“[11]-Anwendungen, wie beispielsweise Luminous von Aleph Alpha oder ChatGPT 3.5 oder 4 von OpenAI bzw. Microsoft, in einer Behörde eingesetzt, werden bereits vollständig austrainierte Anwendungen von den jeweiligen Herstellern erworben und in die eigene Anwendungsumgebung gebracht. Sie können damit grundsätzlich ohne weitere Justierungen in einer IT-Umgebung eingesetzt werden. Meist ist es trotzdem erforderlich, die vollständig austrainierte Anwendung an die jeweiligen internen Maßgaben anzupassen und dieser die spezifische Behördensprache beizubringen. In diesen Fällen werden interne Inhalte wie Vermerke, Schreiben oder sonstige relevante Dokumente importiert, damit sie die Struktur, die Sprache und die Besonderheiten lernt und die ausgegebenen Informationen an diese Vorgaben anpassen kann.

Dieser Import ist nach der hier vertretenen Ansicht nicht als Training - siehe Ziffer 4.3 - zu betrachten. Das Training und die Entwicklung sind mit Erwerb der jeweiligen Anwendung bereits abgeschlossen. Die Anwendung ist vollständig austrainiert. Es handelt sich damit um einen dem Training nachgelagerten Prozess. Die Anwendung wird lediglich an die individuellen Voraussetzungen der nutzenden Behörde angepasst und für notwendige Anwendungsfälle optimiert.

Wie bereits unter Ziffer 4.2 dargestellt, ist die KI-Anwendung selbst nach der hier vertretenen Ansicht ein sogenanntes Betriebsmittel. Der Import etwaiger personenbezogener Daten in eine KI-Anwendung stellt damit die Bereitstellung eines Datensatzes dar, der für die Nutzung der KI als Betriebsmittel notwendig, typisch und spezifisch ist.

Rechtsgrundlage für das Anpassen an die individuellen Voraussetzungen der nutzenden Behörde ist damit nach der hier vertretenen Auffassung die Rechtsgrundlage, die auch der Aufgabenerfüllung der Behörde selbst zugrunde liegt, das heißt Art. 6 Abs. 1 UAbs. 1 Buchstabe e,

[11] Franke, Datenschutzrechtskonformes Training von KI-Systemen mit öffentlich verfügbaren personenbezogenen Daten, RDi 2023, 565

Abs. 3 DSGVO in Verbindung mit einer spezialgesetzlichen oder allgemeinen Datenverarbeitungsbefugnis.

Vergleichbar mit anderen Programmen, die der Behörde durch ein Rechenzentrum bereitgestellt werden, ist das Verzeichnis der Verarbeitungstätigkeiten um die KI-Anwendung zu ergänzen.

4.5. Einbindung und Nutzung einer KI-Anwendung in einem eigenen Mandanten[12]

Nutzt eine Behörde eine KI-Anwendung in einem eigenen Mandanten für Verarbeitungstätigkeiten, für die eine Rechtsgrundlage vorliegt, hat sie unter Berücksichtigung und nach Abwägung der Risiken für betroffene Personen zu entscheiden, ob personenbezogene Daten in der Anwendung verarbeitet werden dürfen. Wird die Eingabe und der Import von personenbezogenen Daten untersagt, werden datenschutzrechtliche Risiken deutlich verringert. Um zu verhindern, dass personenbezogene Daten durch Beschäftigte versehentlich in einen Prompt eingegeben werden, müssen entsprechende Sensibilisierungsmaßnahmen als organisatorische Maßnahmen vorgesehen werden. Im Übrigen muss sichergestellt sein, dass die KI-Anwendung keine personenbezogenen Daten enthält und nicht mit Eingaben der Nutzer weitertrainiert wird. Dies muss der Hersteller / Anbieter zusichern. Diese und weitere technische und organisatorische Maßnahmen gemäß Art. 32, 25 DSGVO befinden sich in der Checkliste im Leitfaden für Dienststellen.

4.5.1. Datenschutzrechtliche Verantwortlichkeit

Verantwortlich nach Art. 4 Nr. 7 DSGVO ist, wer allein oder gemeinsam mit einem anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten, also über das „Warum“ und das „Wie“, entscheidet.

Wird eine vollständig austrainierte KI-Anwendung von einer Behörde in ihre Abläufe und Prozesse integriert, ist davon auszugehen, dass die Behörde bei der Nutzung über die Mittel und Zwecke der Datenverarbeitung bestimmt und damit datenschutzrechtlich verantwortlich ist.[13] Der Betreiber der Anwendung wird in der Regel als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO einzustufen sein. Er verarbeitet personenbezogene Daten ausschließlich im Auftrag des Verantwortlichen und

[12] Unter einem eigenen Mandanten ist ein selbstständig administrierbarer Bereich zu verstehen, in welchem eine logische Datentrennung erfolgt. Dieser Mandantenbereich kann sowohl im eigenen Rechenzentrum, als auch beim Hersteller bzw. bei Dritten betrieben werden.

[13] Puschky, Datenschutzrechtliche Hürden bei der Nutzung von KI im Unternehmen, ZD-Aktuell 2023, 01385

ist an die Weisungen des Verantwortlichen gebunden. Um datenschutzrechtlichen Bestimmungen ausreichend nachkommen zu können, ist es zwingend erforderlich, einen Vertrag mit dem Hersteller zur Auftragsverarbeitung nach Art. 28 Abs. 3 S. 1 DSGVO zu schließen.

Bei der inhaltlichen Ausgestaltung der Vereinbarung ist darauf zu achten, dass der Hersteller sich keine Rechte einräumt, die entsprechenden Daten für das weitere Training oder sonstige eigene Zwecke zu verwenden. Zudem sollte sich die Behörde weitgehende Unterstützung bei den von ihr zu erfüllenden Pflichten nach Art. 5 Abs. 2 DSGVO zusichern lassen, etwa in Form von Unterlagen zur Unterstützung bei der Fertigung einer Datenschutz-Folgenabschätzung.

Als Orientierungshilfe dafür, was grundsätzlich beim Abschluss einer Vereinbarung mit großen Cloud-Anbietern zu beachten ist, wird auf die Handreichung des Bayerischen Landesbeauftragten für den Datenschutz vom 01.09.2023 „Microsoft als Auftragsverarbeiter beim Einsatz von Microsoft 365“ verwiesen.[14]

Konstellationen, in denen von einer gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO auszugehen wäre, sind nach dem aktuellen Stand bisher nicht bekannt.

4.5.2. Datenschutzrechtliche Herausforderungen

Behörden als Verantwortliche sind dazu verpflichtet, die datenschutzrechtlichen Grundsätze aus Art. 5 Abs. 1 DSGVO einzuhalten. Die Einhaltung muss gegenüber den jeweiligen Datenschutzaufsichtsbehörden gemäß Art. 5 Abs. 2 DSGVO nachgewiesen werden.

Art. 5 Abs. 1 Buchstabe a DSGVO legt fest, dass Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. Es handelt sich dabei um den sogenannten Transparenzgrundsatz. Um diesen Grundsatz zu wahren, ist das Verzeichnis der Verarbeitungstätigkeiten sowie gegebenenfalls die Datenschutzinformation um die KI-Anwendung zu ergänzen.

Ein Spannungsverhältnis zum Datenschutz kann sich durch das Prinzip der Datensparsamkeit nach Art. 5 Abs. 1 Buchstabe c DSGVO ergeben. Dieses besagt, dass Daten auf das für die Zwecke der Verarbeitung notwendige Maß zu beschränken sind. Es sollten daher möglichst wenig personenbezogenen Daten verarbeitet werden. Technische Maßnahmen wie die Anonymisierungen, aber auch Pseudonymisierungen oder Zugriffsbeschränkungen können helfen, etwaige Risiken für die betroffenen Personen zu verringern.

[14] Der Bayerische Landesbeauftragte für den Datenschutz: Microsoft als Auftragsverarbeiter beim Einsatz von „Microsoft 365“ (Handreichung), Stand: 01.09.2023; Microsoft als Auftragsverarbeiter beim Einsatz von Microsoft 365 (datenschutz-bayern.de)

Soweit Betroffenenrechte nach Art. 15 ff. DSGVO geltend gemacht werden, ist zwischen dem Training durch den Hersteller / Anbieter und dem Fine-Tuning durch die Behörde zu differenzieren: Hat man sich vom Hersteller zusichern lassen, dass die austrainierte KI-Anwendung keine personenbezogenen Daten mehr enthält bzw. verarbeitet, dürfte sich die Frage nach Betroffenenrechten im Hinblick auf Trainingsdaten nicht stellen. Soweit die Behörde zum Fine-Tuning personenbezogene Daten verwendet hat, ist sie Adressatin etwaiger Betroffenenrechte hierzu.

An dieser Stelle kann eine Protokollierung der Prompts und Ausgabeergebnisse bei Anwendungen, die durch Vollautomatisierung ein hohes Risiko für die betroffenen Personen darstellen, wie beispielsweise Anwendungen, die unmittelbaren Kontakt zu Bürgern aufnehmen (Chatbots), dabei unterstützen, einem etwaigen Auskunftsanspruch der betroffenen Person nachzukommen. Die Eingaben von Bürgerinnen und Bürgern sollten dabei allerdings nicht zu lange gespeichert werden, sondern nur solange, wie mit einer Beschwerde über eine etwaige Antwort zu rechnen ist. Auf die Speicherung ist zudem in geeigneter Weise hinzuweisen.

Die DSGVO legt in Art. 22 Abs. 1 fest, dass betroffene Personen nicht ausschließlich einer auf automatisierter Verarbeitung beruhenden Entscheidung unterworfen werden dürfen. Nach neuester Rechtsprechung des EuGH[15] ist das Scoring durch die SCHUFA eine automatisierte Entscheidung, sodass davon ausgegangen werden kann, dass auch ein von einer KI-Anwendung generierter Inhalt als eine automatisierte Entscheidung einzustufen ist. Damit eine betroffene Person nicht ausschließlich einer automatisierten Entscheidung unterworfen wird, ist es zwingend notwendig, dass der jeweilige Beschäftigte das Letztentscheidungsrecht behält, bei seiner Entscheidung gar weitere Faktoren als die von der KI-Anwendung ausgegebenen berücksichtigt und die von der KI-Anwendung generierten Inhalte zwingend auf inhaltliche Richtigkeit und Vollständigkeit überprüft. Auch an dieser Stelle kann es zur Nachvollziehbarkeit etwaiger fehlerhafter Ausgaben – je nach Höhe des Risikos – angezeigt sein, sowohl Prompts, als auch Ausgaben und Datenquellen zu protokollieren und für einen angemessenen Zeitraum zu speichern.

Insbesondere bei der Nutzung von KI-Anwendungen, deren Hersteller aus Drittstaaten wie den USA stammen, ist neben der Einhaltung von Kapitel V der DSGVO darauf zu achten, auf welchen Servern die Daten gespeichert werden, denn eine Speicherung der Daten auf Servern außerhalb der EU bzw. des EWR erfordert die Einhaltung besonderer datenschutzrechtlicher Voraussetzungen. Unabhängig davon werden Daten, wie beispielsweise Meta- und Telemetriedaten, meist trotz Speicherung im europäischen Raum in das jeweilige Drittland übermittelt. Eine solche Übermittlung bedarf geeigneter datenschutzrechtlicher Garantien nach Art. 44 ff. DSGVO. Bei Vorliegen eines Angemessenheitsbeschlusses der Europäischen Kommission ist ein vergleichbares Datenschutzniveau im jeweiligen Drittland anzunehmen. Nach

15 EuGH, Urteil vom 07.12.2023, C-634/21

dem jüngst in Kraft getretenen Angemessenheitsbeschluss der Europäischen Kommission (EU-US-Data Privacy Framework) ist ein vergleichbares Schutzniveau personenbezogener Daten bei Datenübermittlungen von zertifizierten Partnern in die USA anzunehmen. Sollte ein solcher jedoch nicht vorliegen, sind geeignete Garantien wie Standardvertragsklauseln zu treffen, um die Daten bei etwaigen Transfers zu schützen.

Insgesamt ist das Risiko für betroffene Personen möglichst gering zu halten. So ist mittels geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 25 und 32 DSGVO sicherzustellen, dass die Risiken für Betroffene möglichst minimiert werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Für eine Einschätzung des Risikos ist bei dem Einsatz von KI zu prüfen, ob eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO zu erstellen ist. Sollte eine Datenschutz-Folgenabschätzung durchzuführen sein, ist der Einsatz anhand der vorhandenen Risiken zu beurteilen und es sind geeignete Maßnahmen zu treffen, die den Schutz personenbezogener Daten gewährleisten. Geeignete technische und organisatorische Maßnahmen bei der Nutzung von KI werden im Leitfaden für Dienststellen aufgelistet. Als Hilfestellung zur Erstellung einer Datenschutz-Folgenabschätzung wird auf die Orientierungshilfe des Bayerischen Landesbeauftragten für den Datenschutz zur Risikoanalyse und Datenschutz-Folgenabschätzung verwiesen.[16]

4.6. Nutzung frei zugänglicher KI-Anwendungen unmittelbar im Internet

Sollte sich eine Behörde dazu entscheiden, die Nutzung von frei im Internet zugänglichen KI-Anwendungen wie etwa dem Microsoft Bing Co Pilot oder ChatGPT von OpenAI zu erlauben, müssen die datenschutzrechtlichen Bestimmungen ebenfalls beachtet und gegebenenfalls besondere zusätzlichen Schutzmaßnahmen vorgesehen werden. Daneben sollten bei der Auswahl der jeweiligen Anwendung die Qualität der Ergebnisse im Hinblick auf Verlässlichkeit sowie die Frage, ob der Hersteller besondere Mühe darauf verwendet hat, die KI diskriminierungsfrei zu gestalten, berücksichtigt werden. Die Ausgabeergebnisse sind deshalb zwingend auf Diskriminierungsfreiheit sowie inhaltliche Richtigkeit und Vollständigkeit zu überprüfen.

Vor dem Hintergrund, dass entsprechende Anbieter die KI-Anwendung gerade deshalb im Internet zur Verfügung stellen, damit sie die von Nutzern eingegebenen Daten zu Trainingszwecken weiterverwenden können, ist bei einer solchen Nutzung besondere Vorsicht geboten. Sofern die Nutzung einer frei im Internet zugänglichen KI-Anwendung erlaubt wird, sollte die Verarbeitung personenbezogener Daten grundsätzlich untersagt werden. Die in Ziffer 4.5.2 dargestellten datenschutzrechtlichen Herausforderungen können andernfalls nicht bewältigt werden. Die

[16] Der Bayerische Landesbeauftragte für den Datenschutz, Orientierungshilfe zur Risikoanalyse und Datenschutzfolgenabschätzung: Systematik, Anforderungen, Beispiele, Stand: 01.05.2022

Planung und Umsetzung sollte jedenfalls in enger Zusammenarbeit mit den behördlichen Datenschutzbeauftragten erfolgen.

Eine Nutzung solcher KI-Anwendungen sollte daher allenfalls unter der Prämisse erlaubt werden, dass der Anbieter sowohl Opt-Out-Möglichkeiten in den Einstellungen der jeweiligen KI-Anwendung zur Verfügung stellt, um die Nutzung der Daten zu Trainingszwecken und die Speicherung der „History“, also des Verlaufs des Prompts auszuschließen als auch der Beschäftigte von diesen Möglichkeiten Gebrauch macht.

Sollte auch die Nutzung von Anwendungen erlaubt werden, für die man sich zuvor registrieren muss, wird zum Schutz der Daten der Beschäftigten dringend empfohlen, gegebenenfalls besondere E-Mail-Adressen ohne Namen zur Verfügung zu stellen oder die Nutzung von Funktions-E-Mail-Adressen anzuordnen. Bei solchen Anwendungen sollte die IT über etwaige Anmeldungen informiert werden. Zusätzlich sollten, falls möglich, Authentifizierungsverfahren genutzt werden, um Gefahren für eine missbräuchliche Nutzung des Accounts vorzubeugen.

Bei Funktions-E-Mail-Adressen, die von mehreren Beschäftigten gleichzeitig genutzt werden, ist neben den bereits genannten Aspekten besonders darauf zu achten, dass der Prompt-Verlauf nicht gespeichert wird. Ein Beschäftigter sollte nicht die Möglichkeit haben, die vorherigen Eingaben eines anderen Beschäftigten einzusehen.

Die wesentlichen datenschutzrechtlichen Aspekte zur Nutzung einer im Internet frei zugänglichen KI-Anwendung werden in Anlehnung an die vom Hamburgischen Landesbeauftragten für den Datenschutz vorgelegte Checkliste[17] im Leitfaden für Dienststellen zur Verfügung gestellt.

4.7. Schadensersatz nach Art. 82 DSGVO

Der Pflicht zur Überprüfung der Ausgaben einer KI-Anwendung auf inhaltliche Richtigkeit und Vollständigkeit kommt nicht zuletzt vor dem Hintergrund eines möglichen Schadensersatzanspruchs der betroffenen Person nach Art. 82 DSGVO erhebliche Bedeutung zu. Nach neuester Rechtsprechung des EuGH[18] ist insoweit nicht erforderlich, dass Verstöße gegen die DSGVO von Leitungsorganen begangen wurden oder diese Kenntnis von den Verstößen hatten. Die Haftung des Verantwortlichen erstreckt sich auf jedwede Verarbeitung personenbesonderer Daten, die durch ihn oder in seinem Namen erfolgt. Das umfasst auch Verstöße, die durch andere Personen als der Leitung, also von sämtlichen Beschäftigten, herbeigeführt wurden.

[17] https://datenschutz-hamburg.de/news/checkliste-zum-einsatz-llm-basierter-chatbots

[18] EuGH, Urteil vom 05.12.2023, C-807/21

5. Dienst- und verwaltungsrechtliche Aspekte

5.1. Aspekte des Bayerischen Personalvertretungsgesetzes (BayPVG)

Grundsätzlich empfiehlt sich hinsichtlich der (potentiellen) Anwendung von KI zur Erfüllung dienstlicher Aufgaben eine frühzeitige vertrauensvolle Zusammenarbeit mit den zuständigen Personalvertretungen. Darüber hinaus sind die Beteiligungsrechte der Personalvertretung zu wahren. So kann insbesondere eine Maßnahme, soweit sie der Mitbestimmung der Personalvertretung unterliegt, nach Art. 70 Abs. 1 Satz 1 BayPVG nur mit ihrer Zustimmung getroffen werden. Soweit die Personalvertretung an Entscheidungen mitwirkt, ist nach Art. 72 Abs 1 Satz 1 BayPVG eine beabsichtigte Maßnahme vor ihrer Durchführung mit dem Ziel einer Verständigung rechtzeitig und eingehend mit ihr zu erörtern. Bei dem Einsatz von KI zur Erfüllung dienstlicher Aufgaben beziehungsweise Regelungen zum Einsatz von KI können insbesondere die Mitbestimmungsrechte in Art. 75a Abs. 1 Nr. 1 (Einführung, Anwendung und erhebliche Änderung technischer Einrichtungen zur Überwachung des Verhaltens oder der Leistung der Beschäftigten) sowie die die Mitwirkungsrechte gemäß Art. 76 Abs. 1 Satz 1 Nr. 2 (Regelung des Verhaltens der Beschäftigten), Art. 76 Abs. 2 Nr. 1 (Einführung grundlegend neuer Arbeitsmethoden) und/oder auch Art. 76 Abs. 2 Nr. 2 BayPVG (Maßnahmen zur Hebung der Arbeitsleistung und zur Erleichterung des Arbeitsablaufs) einschlägig sein. Dies lässt sich allerdings nicht generell im Voraus sagen, sondern ist stets im Einzelfall und anhand der beabsichtigten Maßnahme oder des Projekts vorab genau zu prüfen. Für die Richter- und Staatsanwaltsräte enthalten Art. 28 Nr. 9, Art. 29 Nrn. 2, 6 und 7, Art. 37 Abs. 1 Satz 1 BayRiStAG entsprechende Beteiligungstatbestände.

Zu beachten ist dabei immer auch die ganz wesentliche Frage, welche Personalvertretung zuständig ist. Nach Art. 80 Abs. 1 BayPVG ist in Angelegenheiten, in denen die Dienststelle zur Entscheidung befugt ist, der bei ihr gebildete Personalrat (örtlicher Personalrat) zu beteiligen. Gemäß Art. 80 Abs. 2 Satz 1 BayPVG ist statt des örtlichen Personalrats die jeweilige Stufenvertretung zu beteiligen, wenn eine übergeordnete Dienststelle Entscheidungen für den gesamten Geschäftsbereich oder für eine oder mehrere nachgeordnete Dienststellen trifft. Im Falle der Vorgabe von Regelungen seitens der obersten Dienstbehörden für die jeweiligen Ressorts ist die bei der jeweiligen obersten Dienstbehörde gebildete Stufenvertretung (HPR) zu beteiligen. Die Zuständigkeiten der Richter- und Staatsanwaltsräte sind in Art. 27 Abs. 2, Art. 37 Abs. 1 Satz 1 BayRiStAG geregelt.

In Abhängigkeit vom einschlägigen Beteiligungstatbestand (z. B. Art. 75a Abs. 1, Art. 76 Abs. 2 Nr. 1 und 2 BayPVG) ist regelmäßig die Arbeitsgemeinschaft der Hauptpersonalräte (ARGE-HPR) anzuhören, wenn entweder die Staatsregierung eine Entscheidung für die Geschäftsbereiche der obersten Dienstbehörden in Form unmittelbar verbindlicher Regelungen trifft (vgl. Art. 81 Abs. 3

Satz 1 Nr. 1 BayPVG) oder bei ressortübergreifenden Maßnahmen einer obersten Dienstbehörde (vgl. Art. 81 Abs. 3 Satz 1 Nr. 2 BayPVG). Etwaige Folgemaßnahmen in den Ressorts unterliegen trotz Beteiligung der Arbeitsgemeinschaft der Hauptpersonalräte ggf. der Beteiligung durch die jeweils zuständigen Personalvertretungen, da gemäß Art. 81 Abs. 4 Satz 3 BayPVG die Befugnisse und Pflichten der Personalvertretungen nicht berührt werden.

5.2. Allgemeine Geschäftsordnung für Behörden des Freistaats Bayern (AGO)

Gemäß § 10 Abs. 1 AGO sollen Vorgänge vorrangig mit Unterstützung von Informations- und Kommunikationstechnik (IuK-Technik) bearbeitet und aufbewahrt werden. Nach § 10 Abs. 1 Satz 2 werden weitere Einzelheiten durch die Ressorts geregelt.

Einschränkend dürfen aufgrund § 10 Abs. 4 AGO dafür im Grundsatz nur dienstliche IT-Ausstattung und freigegebene Programme verwendet werden. Dies impliziert, dass auch der Einsatz von generativer KI nur zulässig ist, sofern eine entsprechende Freigabe vorliegt.

5.3. Gesetz über die Digitalisierung im Freistaat Bayern (Bayerisches Digitalgesetz – BayDiG)

In Art. 5 Abs. 1 BayDiG ist geregelt, dass staatliche Prozesse der Verwaltung des Freistaates Bayern vollständig digitalisiert und bereits digitalisierte Prozesse in einem Verbesserungsprozess fortentwickelt werden sollen.

Nach Art. 5 Abs. 2 Satz 2 BayDiG ist der Einsatz von Künstlicher Intelligenz in der Verwaltung durch „geeignete Rechtsschutz- und Kontrollmechanismen“ abzusichern.

Im Unterschied zum ITEG Schleswig-Holstein (vgl. §§ 4 bis 10 ITEG) verzichtet Art. 5 Abs. 2 Satz 2 BayDiG bewusst auf eine detaillierte gesetzliche Vorgabe der konkreten Rechtsschutz- und Kontrollmechanismen für den KI-Einsatz in der Verwaltung: Aufgrund der Vielzahl möglicher Einsatzgebiete von KI – von der Verarbeitung von Satellitenbildern über die Erstellung von Textzusammenfassungen bis hin zum umfassenden IT-Einsatz bei der Vorbereitung und dem Erlass von Verwaltungsentscheidungen – wurde Art. 5 Abs. 2 Satz 2 BayDiG vielmehr flexibel ausgestaltet, sodass auch zukünftige Entwicklungen abgebildet werden können und seitens der die KI einsetzenden Stelle ein entsprechender tatbestandlicher Beurteilungsspielraum besteht.

Besondere Bedeutung bei der Ausfüllung dieses Beurteilungsspielraumes spielt der AI Act der Europäischen Union. Aus der Begründung des Änderungsantrags (LT-Drs. 18/23580), durch den

Abs. 2 Satz 2 in Art. 5 BayDiG eingeführt wurde, geht hervor, dass bei der Schaffung der Regelung „das aktuelle Rechtsetzungsverfahren auf EU-Ebene im Rahmen des Artificial Intelligence Act berücksichtigt [wurde]“. Dabei geht der Bezug zum AI Act so weit, dass in der Vorschrift auf eine Legaldefinition des Begriffs „KI“ angesichts der Entwicklungsoffenheit und Dynamik der technischen Entwicklungen verzichtet und stattdessen auf die Definition des AI Acts Bezug genommen wurde. Vor diesem Hintergrund sind die im AI-Act etablierten Rechtsschutz- und Kontrollmechanismen besonders zu berücksichtigen; es können jedoch ggfs. auch noch weitere Anforderungen, insbesondere verfassungsrechtlicher Natur, zu berücksichtigen sein.

Zusammenfassend begründet Art 5 Abs. 2 Satz 2 BayDiG damit keine zusätzlichen einfachgesetzlichen Beschränkungen des KI-Einsatzes in der Verwaltung, die sich nicht bereits aus höherrangigem Recht (EU-Recht oder Verfassungsrecht) ergeben.

Art. 12 BayDiG regelt die Rechte in der digitalen Verwaltung. Gemäß Art. 12 Abs. 3 BayDiG ist ein sofortiger Vollzug vollständig automatisiert erlassener Verwaltungsakte nur aufgrund gesetzlicher Ermächtigung zulässig. Beispielhaft kann hier § 155a Abs. 4 der Abgabenordnung genannt werden, der den Finanzbehörden Befugnisse für einen umfassenden IT-Einsatz bei der Steuerfestsetzung einräumt.

Auf Grundlage von Art. 44 Abs. 2 Nr. 3 BayDiG darf das LSI nunmehr ausdrücklich Daten aus öffentlich zugänglichen Quellen erheben und automatisiert auswerten, sofern diese Informationen mit Auswirkungen auf die Sicherheit der Informationstechnik des Landes oder der an das Behördennetz angeschlossenen Stellen enthalten könnten. Datenschutzrechtlich abgesichert werden soll hier insbesondere der Einsatz von Werkzeugen/Diensten im Bereich „Open Source Intelligence (OSINT)“.

5.4. Einschränkung von automatisierten Verfahren

Werden bei einem Einsatz von KI Personalaktendaten verarbeitet, ist Art. 111 BayBG zu beachten. Dieser erklärt den Einsatz von automatisierten Verfahren für die in Art. 103 BayBG genannten Zwecke, also insbesondere zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, grundsätzlich für zulässig. Gleichzeitig zeigt er Grenzen für deren Einsatz auf. Neben dem Grundsatz der Zweckbindung und dem Erforderlichkeitsprinzip ist insbesondere zu berücksichtigen, dass eine beamtenrechtliche Entscheidung nur dann auf einer ausschließlich automatisierten Verarbeitung von personenbezogenen Daten beruhen darf, wenn einem vorausgegangenen Antrag des Beamten oder der Beamtin vollständig entsprochen wird.

5.5. Bürgerliches Gesetzbuch (BGB) i. V. m. Grundgesetz (GG) - Amtshaftung

Gemäß § 839 BGB i. V. m. Art. 34 GG ist der Staat oder die Körperschaft, in deren Dienst eine Beamtin oder ein Beamter eine ihr beziehungsweise ihm obliegende Amtspflicht verletzt, haftbar, wobei bei Vorsatz oder grober Fahrlässigkeit ein Rückgriff vorbehalten bleibt.

5.6. § 37 BeamtStG (Verschwiegenheitspflicht)

Nach § 37 BeamtStG haben Beamtinnen und Beamte über die ihnen bei oder bei Gelegenheit ihrer amtlichen Tätigkeit bekannt gewordenen dienstlichen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt auch über den Bereich eines Dienstherrn hinaus sowie nach Beendigung des Beamtenverhältnisses. Eine Ausnahme gilt unter anderem dann, wenn Tatsachen mitgeteilt werden, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

Die Verschwiegenheitspflicht ist insbesondere bei Eingaben in den Prompt einer KI zu berücksichtigen, sofern die Daten durch das KI-Anwendung zu Trainingszwecken genutzt werden.

5.7. Verschlusssachenanweisung für die Behörden des Freistaates Bayern (VSA)

Die Anforderungen an den materiellen Geheimschutz nach der Verschlusssachenanweisung für die Behörden des Freistaates Bayern (VSA) müssen eingehalten werden.

5.8. Disziplinarrechtliche Erwägungen

Verstößt eine Beamtin oder ein Beamter beim Umgang mit KI-Systemen schuldhaft gegen eine Dienstpflicht, stellt dies gem. § 47 Abs. 1 BeamtStG ein Dienstvergehen dar, das disziplinarrechtlich geahndet werden kann. Je nach den Umständen des Einzelfalles kann sogar die Entfernung aus dem Beamtenverhältnis gerechtfertigt sein.