KARL
Künstliche Intelligenz für Arbeit und Lernen

KARL – Rechtliche Aspekte

Sowohl im Rahmen der Erforschung und Entwicklung eines KI-Systems als auch bei der Einführung eines solchen im Betrieb sollten rechtliche Aspekte nicht vernachlässigt werden. Welche Rechtsfragen tangiert sind, entscheidet sich vornehmlich nach dem Einsatzkontext sowie betroffenen Daten und potentiellen Folgen und Risiken.

Anknüpfungspunkt	**Rechtsgebiet / Gesetze**	**Zuständige Rollen** (sofern vorhanden)
Verarbeitung personenbezogener Daten	Datenschutzrecht (DSGVO, BDSG, LDSG, etc.)	Datenschutzbeauftragte/r, ggf. Betriebsrat
Telekommunikation / Telemedien	TTDSG, TKG	Datenschutzbeauftragte/r
Bestimmte Angelegenheiten Arbeitsorganisation	Arbeitsrecht (BetrVG)	Betriebsrat
Geistiges Eigentum (Texte, Bilder, Datenbanken,....)	Urheberrecht (UrhG)	Rechtsabteilung / Compliance-Beauftragter
Geschäftsgeheimnisse	GeschGehG	Geheimnisbeauftrage/r
Materielle & immaterielle Schäden durch System	Haftungsrecht (BGB, ProdHaftG, etc.)	Rechtsabteilung / Compliance-Beauftragte/r
KI-System	Künftig: KI-Verordnung (Entwurf der EU-Kommission)	

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Kompetenzzentren Arbeitsforschung

Für die Entwicklung von **standardisierten Vorgehensmodellen** für Software-Entwicklungsprozesse, wie sie in KARL diskutiert werden, sollte danach differenziert werden, welche Rollen sowie ggf. intern vorhandene oder extern hinzuzuziehende Expertisen in welchen Stadien und zu welchen Arbeitsschritten beratend hinzugezogen werden sollten oder zwingend eingebunden werden müssen.

Datenschutzrecht

Die datenschutzkonforme Verarbeitung personenbezogener Daten bei der Planung, Entwicklung, Umsetzung und im Betrieb eines KI-Systems bedarf der umsichtigen und vorausschauenden Organisation, indem datenschutzrechtliche Anforderungen bei der Systementwicklung von Anfang an mitgedacht werden und relevante Fachverantwortliche, wie der/die Datenschutzbeauftragte und ggf. der Betriebsrat, von Beginn an beteiligt werden.

Datenschutzrechtliche Pflichten greifen bei der Verarbeitung **personenbezogener Daten** [1]. Eine erste Weichenstellung bei der Entwicklung KI-basierter Systeme ist die Feststellung des Personenbezugs durch Analyse der Art der Daten und der geplanten Datenflüsse sowie die Entscheidung, ob dieser Personenbezug für die Zielerreichung erforderlich bzw. unvermeidlich ist oder ob über eine **Anonymisierung** die „Flucht aus dem Datenschutzrecht“ angetreten werden soll. Gerade bei der Verarbeitung großer Datenmengen aus unterschiedlichen Quellen sind die Risiken einer Identifizierbarkeit regelmäßig zu (re-)evaluieren, da mit zunehmenden technischen Möglichkeiten auch die Zuordnung von Daten zu einer identifizierbaren Person steigen können [2].

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung
Kompetenzzentren
Arbeitsforschung

Im nächsten Schritt steht die Identifizierung des anwendbaren Rechts. Mit der Datenschutz-Grundverordnung (DSGVO) wurde das Datenschutzrecht weitgehend EU-weit harmonisiert, allerdings sind aufgrund von Öffnungsklauseln und Übergangsregeln in bestimmten Fällen Vorschriften des Bundesdatenschutzgesetzes (BDSG), der Landesdatenschutzgesetze oder des Telekommunikations-und-Telemedien-Datenschutzgesetzes (TTDSG) anwendbar [3], [4]. Bei Letzterem gilt zu bedenken, dass dieses auch nicht-personenbezogene Daten einbezieht. Datenschutzrechtliche Vorschriften können sich auch aus dem jeweils einschlägigen Fachrecht ergeben, wie bspw. dem Messstellenbetriebsgesetz (MsbG) im Bereich der Energieversorgung.

Für eine strukturierte Umsetzung der vielschichtigen Vorgaben bietet sich die Systematisierung anhand der zentralen **Datenschutzgrundsätze** an: Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht. Das Fundament bildet dabei die Festlegung eines Verarbeitungszwecks, an dem sich die Erforderlichkeit der Datenverarbeitung messen muss [5]. Die Beschränkung auf erforderliche Daten ergibt sich schon aus dem Datenminimierungsgrundsatz. Bereits bei der Gestaltung von technischen Systemen sollte die Verarbeitung von Daten mit Personenbezug, soweit technisch möglich und wirtschaftlich zumutbar begrenzt oder ganz vermieden werden.

Aufgrund des der DSGVO zugrundeliegenden **risikobasierten Ansatzes**, insbesondere im Hinblick auf die Konzepte Privacy by Design und by Default [6], Datensicherheit sowie der vom Risiko abhängigen Notwendigkeit eine Datenschutz-Folgenabschätzung [7] durchzuführen, kann die

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Kompetenzzentren Arbeitsforschung

datenschutzrechtliche Bewertung bereits im Rahmen der Entwicklung Anpassungen des KI-Systems im Hinblick auf **technische und organisatorische Maßnahmen** erforderlich machen. Insofern bietet sich ein iterativer Prozess der Konkretisierung rechtlicher Anforderungen als nicht-funktionale Anforderungen, sowie die regelmäßige Re-Evaluierung der Maßnahmen an.

Im Forschungskontext können Forschungsprojekte wie KARL von einigen Privilegien profitieren: so bestehen gewisse Spielräume u.a. im Rahmen der Einwilligung, Zweckbindung, Transparenz und Speicherbegrenzung. Allerdings ist die Reichweite dieser Regelungen teils noch umstritten [8]–[10].

Arbeitsrecht

Vom Arbeitgeber sind neben der Einhaltung der speziellen Datenschutzvorschriften im Beschäftigungskontext auch die **Mitbestimmungsrechte** nach Betriebsverfassungsgesetz (BetrVG) zu beachten. Hierbei kann es sich anbieten, eine **Betriebsvereinbarung** nach Art. 88 Abs. 2 DSGVO iVm § 26 Abs. 4 BDSG zu schließen, um eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten zu schaffen [11]. Der Betriebsrat hat gemäß § 80 Abs. 1 Nr. 1 BetrVG zu überwachen, dass die Vorschriften der DSGVO und des BDSG eingehalten werden, woraus sich für den Betriebsrat aus § 80 Abs. 2 BetrVG ein allgemeiner **Informationsanspruch** ergibt.

Betrifft ein geplanter KI-Einsatz unterschiedliche Aspekte der Arbeitsorganisation, können **Unterrichtungs-, Beratungs-** oder **Mitbestimmungsrechte** des Betriebsrats eröffnet sein. Mitbestimmungspflichtige Aspekte sind u.a. in § 87 BetrVG gelistet: (1) Fragen der Ordnung des Betriebs und des

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung
Kompetenzzentren
Arbeitsforschung

Verhaltens der Arbeitnehmer im Betrieb; (2) Arbeitszeit / Verteilung der Arbeitszeit; (3) vorübergehende Verkürzung oder Verlängerung der betriebsüblichen Arbeitszeit; (4) Zeit, Ort und Art der Auszahlung der Arbeitsentgelte; (5) allgemeine Urlaubsgrundsätze / Urlaubsplans; (6) technische Einrichtungen, die objektiv geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen; (7) Verhütung von Arbeitsunfällen und Berufskrankheiten / Gesundheitsschutz; (8) Sozialeinrichtungen; (9) Betriebswohnungen; (10) Lohngestaltung; (11) Akkord- und Prämiensätze / leistungsbezogener Entgelte; (12) betriebliche Vorschlagswesen; (13) Gruppenarbeit; (14) mobile Arbeit. Der Aspekt der Künstlichen Intelligenz wurde jüngst klarstellend bezüglich der Unterrichtungs- und Beratungsrechte des Betriebsrats über die Planung von Arbeitsverfahren und Arbeitsabläufen in § 90 BetrVG sowie bezüglich der Mitbestimmung bei Auswahlrichtlinien in § 95 BetrVG aufgenommen. Somit wird sichergestellt, dass die Pflichten der Arbeitgeber und Rechte des Betriebsrats weiterhin gelten, auch wenn KI zum Einsatz kommt [12], [13]. Weiter besteht ein Mitbestimmungsrecht des Betriebsrates gemäß § 94 BetrVG bei Personalfragebögen und Beurteilungsgrundsätzen in Verbindung mit einem KI-System. [13] Unterrichtungs- und Beratungsrechte bestehen zudem bei Einführung grundlegend neuer Arbeitsmethoden (§ 111 BetrVG).

Damit der Betriebsrat seine Beratungs- und Mitbestimmungsrechte tatsächlich wahrnehmen kann, sollte die Einbindung rechtzeitig vor einem geplanten KI-Einsatz erfolgen sowie Unterlagen zur Funktionsweise umfassen [13]. Muss der Betriebsrat zur Durchführung seiner Aufgaben die Einführung oder Anwendung von Künstlicher Intelligenz beurteilen, gilt insoweit die Hinzuziehung eines Sachverständigen als

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung
Kompetenzzentren
Arbeitsforschung

erforderlich. Eine Definition des Begriffs „Künstliche Intelligenz“ enthält das BetrVG allerdings nicht.[12], [13]

Sollen KARL-Sachverhalte bereits in realen Umgebungen erprobt werden oder Leitlinien und Hilfestellungen für einen späteren Praxiseinsatz bieten, sollten Abstimmungsprozesse von Beginn an mitgedacht werden. Wie diese praktisch umgesetzt werden könnten, wird im Abschnitt zum **„Moderierten Spezifikationsdialog“** als Instrument antizipierender Technikeinführung beschrieben.

Urheberrecht

Je nachdem welche Datenquellen zum Training von KI-Systemen herangezogen werden sollen, können Urheber- und Leistungsschutzrechte tangiert sein. Im Folgenden werden typische Beispiele beschrieben:

- **Textdokumente** sind sofern es sich um persönlich geistige Schöpfungen handelt urheberrechtlich geschützt, ausgenommen sind amtliche Werke, wie Gesetze, Verordnungen und Bekanntmachungen. Dem/der Schöpfer:in des Werkes stehen bestimmte Verwertungsrechte zu, an denen Nutzungsrechte eingeräumt werden können. Das Urheberrecht erlischt siebzig Jahre nach dem Tode des/der Urheber:in.
- **Bilder und Videos** können als geistige Schöpfung wie Textwerke urheberrechtlichen Schutz genießen. Daneben sind sie als Lichtbilder[1] und Erzeugnisse, die ähnlich wie Lichtbilder hergestellt werden, für 50 Jahre

[1] Unter Lichtbildern werden Abbildungen verstanden, die „dadurch entstehen, dass strahlungsempfindliche Schichten chemisch oder physikalisch durch Strahlung eine Veränderung erfahren“ [14]§ 72 Rn. 11

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Kompetenzzentren Arbeitsforschung

geschützt, wobei das Recht dem/der Lichtbildner:in zukommt.

- **Datenbanken** werden bei individueller Schöpfungshöhe bezüglich Auswahl oder Anordnung der Elemente als Datenbankwerke und damit selbstständiges Werk geschützt. Der/die Datenbankhersteller:in ist darüber hinaus geschützt, wenn die Elemente der Datenbank systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert.
- **Computerprogramme** genießen bei individuell-geistiger Leistung ebenfalls Schutz. Dies gilt allerdings nicht für dem Programm zugrunde liegende Ideen und Grundsätze. Die zustimmungsbedürftigen Handlungen und Ausnahmen sind gesondert, abweichend von den anderen Werkkategorien geregelt.

Bestimmte Nutzungsarten werden gesetzlich erlaubt, hierzu zählen Nutzung für Wissenschaft und Lehre wie auch kommerzielle Nutzungen in gesetzlich definierten Fällen (Schranken des Urheberrechts). Im KARL-Kontext relevant ist die gesetzlich erlaubte Nutzung zum **Text und Data Mining (TDM)**, wobei zwischen Forschungszwecken und sonstigen Zwecken unterschieden wird. TDM ist die automatisierte Analyse von einzelnen oder mehreren digitalen oder digitalisierten Werken, um daraus Informationen insbesondere über Muster, Trends und Korrelationen zu gewinnen. [15]

Text und Data Mining für Zwecke der wissenschaftlichen Forschung: die Norm berechtigt zunächst Forschungsorganisationen Werke auch ohne Zustimmung zu vervielfältigen, sofern sie nicht kommerzielle Zwecke verfolgen, sämtliche

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Kompetenzzentren Arbeitsforschung

Gewinne in die Forschung reinvestieren oder im Rahmen eines staatlich anerkannten Auftrags im öffentlichen Interesse tätig sind. Für die Kooperation mit Dritten, wie privaten Unternehmen, dürfen in bestimmten Fällen Werke zugänglich gemacht werden. Zudem sollen diese sicher verwahrt werden.[16]

Text und Data Mining: in sonstigen Fällen sind Vervielfältigungen im Rahmen des TDM zulässig bei rechtmäßig zugänglichen Werken. Der/die Rechtsinhaber:in kann sich allerdings vorbehalten, dass diese Nutzungen ausgeschlossen sind. Bei online zugänglichen Werken muss dieser Nutzungsvorbehalt in maschinenlesbarer Form erfolgen.

Bei Open-Source-Projekten bzw. als Open Data bereitgestellten Daten werden zumeist über die Lizenzen Rechte zur Vervielfältigung und Bearbeitung gewährt. Diese können allerdings mit unterschiedlichen Bedingungen versehen sein, insbesondere die unter Nutzung der Lizenzen entstandenen Werke ebenfalls zur freien Nutzung zur Verfügung zu stellen (sog. Copy-Left).

Schutz von Geschäftsgeheimnissen

Daten können neben als auch ohne Personenbezug auch bei Unternehmensbezug rechtlichen Schutz genießen. Dies ist der Fall, wenn diese Daten nicht allgemein bekannt oder nicht ohne Weiteres zugänglich sind und daher von wirtschaftlichem Wert sind, die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber sind und bei der ein berechtigtes Interesse an der Geheimhaltung besteht [17], [18]. Das Gesetz unterscheidet zwischen explizit erlaubten Handlungen, Handlungsverboten und Ausnahmen. Zu den erlaubten

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Kompetenzzentren Arbeitsforschung

Handlungen zählt mittlerweile das Reverse Engineering. Ausnahmen gelten insbesondere für Whistleblower [19].

Zu Überlappungen mit dem Datenschutzrecht kommt es, wenn Geschäftsgeheimnisse ebenfalls über Personenbezug verfügen. Organisatorische und technische Schutzmaßnahmen erfüllen dann eine Doppelfunktion, da Geschäftsgeheimnisse per Definition **angemessene Geheimhaltungsmaßnahmen** erfordern [20]. Während das Datenschutzrecht zwingende Vorgaben enthält, erfolgt der Schutz von Geschäftsgeheimnissen zumeist im Eigeninteresse, um wertvolles Know-How des Unternehmens nicht nach außen zu offenbaren. Daneben können vertragliche Verpflichtungen den Schutz der Geschäftsgeheimnisse Dritter erforderlich machen.

Sonstige Haftungsfragen

Sollen KI-Systeme in der Praxis eingesetzt werden bzw. für den Praxiseinsatz vertrieben werden, sollten sich Entwickler:innen und Anbieter:innen stets potentiellen Haftungsrisiken bewusst sein. Zudem wurden mit der Novelle des Verbraucherschutzrechts Herstellerpflichten zur **Aktualisierung**, d.h. Bereitstellung von Software-Updates, etabliert [21], [22]. Die folgende Tabelle zeigt, in welchen Situationen bestimmte Haftungsfragen näher geprüft werden sollten.

Bereich	Voraussetzungen	Haftungsrisiken
Vertragliche Haftung (B2B)	Verträge über die Bereitstellung von Software können insbes. unter das Kauf-, Miet-, Werk- oder	Haftung für Mängel beim Kaufvertrag: Abweichung von subjektiven oder objektiven Anforderungen: - Vereinbarte Beschaffenheit über Art, Menge,

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Kompetenzzentren Arbeitsforschung

	Dienstvertragsrecht fallen – oftmals liegen typengemischte Verträge vor.	Qualität, Funktionalität, Kompatibilität, Interoperabilität - Eignung nach der im Vertrag vorausgesetzten Verwendung - Erwartbares / vereinbartes Zubehör / Anleitung vorhanden & korrekt - Eignung für gewöhnliche Verwendung - Übliche Beschaffenheit, insbes. Haltbarkeit, Funktionalität, Kompatibilität und Sicherheit - Entsprechung Muster / Testversion
Verbraucherverträge (B2C): Verbraucher sind natürliche Personen, die Rechtsgeschäfte zu privaten Zwecken abschließen	**Digitale Produkte:** - digitale Inhalte: Daten, die in digitaler Form erstellt und bereitgestellt werden. - digitale Dienstleistungen: die dem Verbraucher Verarbeitung von Daten in digitaler Form oder den Zugang zu solchen Daten ermöglichen, oder die gemeinsame Nutzung in digitaler Form hochgeladenen / erstellten Daten oder sonstige Interaktionen mit diesen Daten ermöglichen.	- Haftung für Mängel bei Abweichung von objektiven oder subjektiven Anforderungen (s.o.) - Aktualisierungspflichten: für einen festgelegten Bereitstellungszeitraum oder vernünftigerweise erwartbaren Zeitraum (Ausnahme: Verbraucher unterlässt Installation)
	Waren mit digitalen Elementen: Sachen,	Haftung für Mängel bei Abweichung von objektiven

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Kompetenzzentren Arbeitsforschung

	die ein digitales Produkt enthalten ohne welches sie ihre Funktion nicht erfüllen	oder subjektiven Anforderungen (s.o.) sowie Nichtbereitstellung Aktualisierungen (s.o.)
Produkthaftung	Hersteller haftet verschuldensunabhängig für von Produktfehlern verursachte Schäden (nicht Schäden am Produkt selbst)	Jemand wird durch den Fehler eines Produkts getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, die für den privaten Ge- oder Verbrauch bestimmt & genutzt wird
Produzentenhaftung	Hersteller haftet für **Konstruktions-, Fabrikations-** und **Instruktionsfehler** sowie die Verletzung der **Produktbeobachtungspflicht**, es sei denn es gelingt der Nachweis fehlenden Verschuldens	Haftung für vorsätzliche oder fahrlässige Verletzung von Leben, Körper, Gesundheit, Freiheit, Eigentum oder ein sonstiges Recht eines anderen. Zu sonstigen Rechten zählt u.a. das allgemeine Persönlichkeitsrecht.

In bestimmten, besonderen Konstellationen können sich Haftungsfragen aus weiteren Regelungen ergeben, wie bspw. dem Straßenverkehrsrecht bei KI-Systemen im Rahmen des automatisierten Fahrens (Halterhaftung, Fahrerhaftung). Einige Normen, bspw. aus dem Strafrecht, wirken darüber hinaus als Schutzgesetze, deren Verletzung zivilrechtlich verfolgt werden kann (bspw. § 303a StGB Datenveränderung).

Künftige KI-Regulierung

Künstliche Intelligenz soll nach Ansicht der EU-Kommission künftig auf EU-Ebene rechtlich reguliert werden. Allerdings betreffen nicht alle Anforderungen sämtliche KI-Systeme

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Kompetenzzentren Arbeitsforschung

gleichermaßen, sondern entscheidend ist das damit verbundene Risiko für die Grundrechte potentiell betroffener Personenkreise. Insofern werden KI-Systeme im aktuellen Entwurf[2] eingeteilt in:

- **Verbotene Praktiken:** KI-Systeme mit Schadenspotential und unbewusst manipulierendem Charakter oder Ausnutzung der Schutzbedürftigkeit von Personen, mithin einem unannehmbaren Risiko sowie biometrische Echtzeit-Fernidentifizierungssysteme
- **Hochrisiko KI-Systeme:** Systeme, die unter bestimmte Rechtsvorschriften der EU fallende Produkte oder Sicherheitskomponenten in solchen Produkten sind und eine Konformitätsbewertung erfordern oder im Bereich biometrische Identifizierung / Kategorisierung, Kritische Infrastrukturen, allgemeine / berufliche Bildung, Beschäftigung, Personalmanagement / Selbstständigkeit, Zugang zu privaten / öffentlichen Diensten / Leistungen, Strafverfolgung, Migration, Asyl und Grenzkontrolle, Rechtspflege und demokratische Prozesse eingesetzt werden.
- **KI-Systeme:** werden im Entwurf der EU zur KI-Verordnung definiert als: „eine Software, die mit einer oder mehreren der in Anhang I [der KI-Verordnung] aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder

[2] 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 vom 21.4.2021.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Kompetenzzentren Arbeitsforschung

Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren“ Anhang I des Entwurfs nennt wiederum zahlreiche Techniken und Konzepte, wie die des maschinellen Lernens, Logik- und wissensgestützte Konzepte als auch statistische Ansätze. Insbesondere die Weite des gewählten Rahmens unter Verweis auf einen Anhang hat vielfache Kritik provoziert [23]–[25].

Für Hochrisiko-KI-Systeme sind zahlreiche Schutzmechanismen vorgesehen, wie ein Risikomanagementsystem, Qualitätsmanagementsystem, menschliche Aufsicht, Transparenz, technische Dokumentation und Aufzeichnungspflichten, Daten & Daten Governance, technische und organisatorische Maßnahmen zu Genauigkeit, Robustheit & Cybersicherheit sowie Konformitätserklärung /-bescheinigung & -kennzeichnung und Registrierungen. Für gewöhnliche KI-Systeme gelten lediglich Transparenzregeln, sodass ersichtlich sein muss, dass es sich um eine KI und keinen Menschen handelt (bspw. bei Chatbots, Deepfakes, etc.).

Gegenstand andauernder Diskussionen ist die Frage, ob mit diesem Entwurf die im Abschnitt **„Warum Ethik in KARL“** aufgeworfenen sozialen, ethischen und gesellschaftspolitischen Herausforderungen einer ausgewogenen rechtlichen Regulierung unterworfen werden, um rechtliche Impulse hin zur Entwicklung menschzentrierter, transparenter, lernförderlicher *und* nachhaltigen KI-Systeme zu setzen. Wichtige Kritikpunkte sind die geringe Adressierung der von den Risiken betroffenen Personen sowie die Verwendung zahlreicher unbestimmter Begriffe, die einen weiten Interpretationsspielraum belassen und damit mit der Befürchtung von Rechtsunsicherheit einhergehen [23]–[27]. So wird deutlich, dass es keine

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung
Kompetenzzentren
Arbeitsforschung

generalisierte Gestaltung von KI geben kann, sondern stets die Dimensionen des Einsatzkontextes, Bandbreiten der Einsatzzwecke, ökologische Implikationen und Beziehungen der betroffenen Personenkreise in die Betrachtung einbezogen werden sollten.

Quellen

[1] Artikel-29-Datenschutzgruppe, „Stellungnahme 4/2007 zum Begriff ‚personenbezogene Daten' - WP 136", Artikel-29-Datenschutzgruppe, Brüssel, Juni 2007. Zugegriffen: 31. August 2018. [Online]. Verfügbar unter: https://www.lda.bayern.de/media/wp136_de.pdf

[2] Artikel-29-Datenschutzgruppe, „Stellungnahme 5/2014 zu Anonymisierungstechniken - WP 216", Brüssel, Apr. 2014. Zugegriffen: 10. November 2018. [Online]. Verfügbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

[3] J. Kühling *u. a.*, *Die Datenschutz-Grundverordnung und das nationale Recht: erste Überlegungen zum innerstaatlichen Regelungsbedarf*. Münster: Verlagshaus Monsenstein und Vannerdat, 2016.

[4] DSK - Datenschutzkonferenz, „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021)", Dez. 2021.

[5] Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on Purpose Limitation - WP 203", Brüssel, Apr. 2013. Zugegriffen: 19. Oktober 2018. [Online]. Verfügbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung
Kompetenzzentren
Arbeitsforschung

[6] European Data Protection Board, „Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0“, Brüssel, Okt. 2020.

[7] DSK - Datenschutzkonferenz, „Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO“, Dez. 2018. Zugegriffen: 20. Mai 2020. [Online]. Verfügbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf

[8] F. Molnár-Gábor, „Die Regelung der wissenschaftlichen Forschung in der DSGVO“, *DSRITB*, S. 159–173, 2018.

[9] A. Roßnagel, „Datenschutz in der Forschung“, *ZD*, S. 157–164, 2019.

[10] T. Weichert, „Die Forschungsprivilegierung in der DS-GVO“, *ZD*, S. 18–24, 2020.

[11] J. Holthausen, „Big Data, People Analytics, KI und Gestaltung von Betriebsvereinbarungen – Grund-, arbeits- und datenschutzrechtliche An- und Herausforderungen“, *RdA*, S. 19–32, 2021.

[12] O. Reinartz, „Das Betriebsrätemodernisierungsgesetz“, *NZA-RR*, S. 457–470, 2021.

[13] J. Frank und M. Heine, „Künstliche Intelligenz im Betriebsverfassungsrecht“, *NZA*, S. 1448–1452, 2021.

[14] H. Ahlberg, H.-P. Götting, und A. Lauber-Rönsberg, Hrsg., *Beck'scher Online-Kommentar zum Urheberrecht*, Bd. 34. Edition. München: C.H. Beck, 2022. Zugegriffen: 11. Juni 2016. [Online]. Verfügbar unter: https://beck-online.beck.de/?vpath=bibdata/komm/BeckOK_UrhR_10/cont/BeckOK.UrhR.htm

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Kompetenzzentren Arbeitsforschung

[15] B. Raue, „Das Urheberrecht der digitalen Wissen(schaft)sgesellschaft“, *GRUR*, S. 14, 2017.

[16] F. Kleinkopf, J. Jacke, und M. Gärtner, „Text- und Data-Mining“, *MMR*, S. 196–200, 2021.

[17] M. Dann und J. Markgraf, „Das neue Gesetz zum Schutz von Geschäftsgeheimnissen“, *NJW*, S. 1774–1779, 2019.

[18] A. Ohly, „Das neue Geschäftsgeheimnisgesetz im Überblick“, *GRUR*, S. 441–451, 2019.

[19] C. Alexander, „Geheimnisschutz nach dem GeschGehGE und investigativer Journalismus“, *AfP*, S. 1–11, 2019.

[20] P. Gola, „Das Geschäftsgeheimnisgesetz und die Datenschutz-Grundverordnung: Parallele Regelungen mit neuen Verpflichtungen und Aufgaben für Datenschutzbeauftragte?“, *DuD*, Bd. 43, Nr. 9, S. 569–574, Sep. 2019, doi: 10.1007/s11623-019-1165-8.

[21] C. Felsch, J. Kremer, und F. Jacoby, „Handhabung der neuen Aktualisierungspflicht bei digitalen Produkten“, *MMR*, S. 18–23, 2022.

[22] J. Kühner und C. Piltz, „Die Updatepflicht für Unternehmen in Umsetzung der Digitale Inhalte Richtlinie — Der Regelungsmechanismus im Referentenentwurf des BMJV v. 3.11.2020 zur Umsetzung der Richtlinie 2019/770/EU“, *CR*, Bd. 37, Nr. 1, S. 1–7, Jan. 2021, doi: 10.9785/cr-2021-370106.

[23] A. Ebert und I. Spiecker gen. Döhmann, „Der Kommissionsentwurf für eine KI-Verordnung der EU“, *NVwZ*, Nr. 16, S. 1188–1193, 2021.

[24] M. Ebers, V. R. S. Hoch, F. Rosenkranz, H. Ruschemeier, und B. Steinrötter, „Der Entwurf für eine EU-KI-Verordnung:

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Kompetenzzentren Arbeitsforschung

Richtige Richtung mit Optimierungsbedarf“, *RDi*, Bd. 3, Nr. 11, S. 528, Nov. 2021.

[25] Europäischer Wirtschafts- und Sozialausschuss und Christa Schweng, „Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zum ‚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 – 2021/106(COD))“. 22. Dezember 2021.

[26] Europäischer Datenschutzausschuss und Europäischer Datenschutzbeauftragter, „EDSA-EDSB Gemeinsame Stellungnahme 5/2021 zum 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“. 18. Juni 2021. Zugegriffen: 30. Mai 2022. [Online]. Verfügbar unter: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_de

[27] A. Sesing und A. Tschech, „AGG und KI-VO-Entwurf beim Einsatz von Künstlicher Intelligenz“, *MMR*, S. 24–30, 2022.

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung
Kompetenzzentren
ArbeitsForschung