

Dr. Patrick Grosmann



Datenschutz

Vivien Lauren Wale



Die Relevanz von Künstlicher Intelligenz im HR-Management

Die Anforderungen von KI-Verordnung und DSGVO im Fokus

Was früher mühsam per Hand erledigt wurde – etwa die Sichtung von Bewerbungen oder die Auswertung von Leistungsdaten – kann heute oft durch KI-Systeme automatisiert werden. KI-Systeme versprechen mehr Effizienz, schnellere Abläufe und objektivere Entscheidungen. Gleichzeitig rechtlich herausfordernd ist dabei die Erfüllung der Anforderungen von Datenschutz-Grundverordnung (DSGVO) und KI-Verordnung (KI-VO).

1 Die rechtlichen Grundlagen – zwischen DSGVO und KI-VO

1.1 Die DSGVO

Die DSGVO bildet den zentralen Rechtsrahmen für den Umgang mit personenbezogenen Daten. Dazu zählen „klassische“ Angaben wie Name, Geburtsdatum oder E-Mail-Adresse ebenso wie vollständige Bewerbungsunterlagen. Die folgenden grundlegenden datenschutzrechtlichen Anforderungen sind zu erfüllen.

1.1.1 Verantwortlichkeit

Für die Datenverarbeitung verantwortlich ist im HR-Bereich meist der Arbeitgeber, da dieser die Zwecke und Mittel der Verarbeitung festlegt.¹ Externe Anbieter, beispielsweise von Bewerbermanagementsystemen, handeln in der Regel als Auftragsverarbeiter und müssen die Vorgaben ebenfalls einhalten. Bei einem Training des KI-Systems ist zudem zwischen einer eigenen Verantwortlichkeit des Softwareanbieters und einer gemeinsamen Verantwortlichkeit abzugrenzen.²

¹ Vgl. Hersemeyer/Ludolph, Datenschutzrechtliche Herausforderungen beim Einsatz Künstlicher Intelligenz im Unternehmenskontext, DSRITB 2023, 365, 367.

² Vgl. Golland, EuZW 2024, 846, 848.

1.1.2 Rechtsgrundlagen der Datenverarbeitung

Die Verarbeitung personenbezogener Daten erfordert stets eine Rechtsgrundlage. In der Praxis stützt sich die Verarbeitung personenbezogener Daten häufig auf die Einwilligung der betroffenen Person (siehe Art. 6 Abs. 1 S. 1 lit. a) DSGVO), die Erfüllung eines Vertrags oder die Durchführung vorvertraglicher Maßnahmen (siehe Art. 6 Abs. 1 S. 1 lit. b) DSGVO) sowie auf die Wahrung berechtigter Interessen (siehe Art. 6 Abs. 1 S. 1 lit. f) DSGVO). Werden besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO verarbeitet, müssen zusätzlich die darin festgelegten strengeren Anforderungen beachtet werden. Faktisch kommt jedoch regelmäßig nur die ausdrückliche Einwilligung in Betracht.

Nationale Gesetze zum Beschäftigtendatenschutz, wie § 26 Bundesdatenschutzgesetz (BDSG) oder die darauf beruhenden landesrechtlichen Bestimmungen, dürfen nur herangezogen werden, wenn sie die Anforderungen und Grenzen des Art. 88 Abs. 1, 2 DSGVO erfüllen. Der EuGH hat innerhalb eines Vorabentscheidungsverfahrens entschieden, dass dies bei § 26 Abs. 1 S. 1 BDSG nicht der Fall ist.³ Da dies bisher nicht abschließend geklärt ist, werden die weiteren Bestimmungen des § 26 BDSG in der Praxis gleichwohl weiterhin angewandt und sind für Arbeitgeber nach wie vor von erheblicher Bedeutung.

Besondere Anforderungen gelten für die Einwilligung im Arbeitsverhältnis: Diese ist nur wirksam, wenn sie freiwillig erteilt wird und in der Regel schriftlich oder elektronisch vorliegt (§ 26 Abs. 2 BDSG). Die Freiwilligkeit ist wegen des Abhängigkeitsverhältnisses besonders kritisch zu prüfen. Entscheidend sind die Umstände der Abgabe, etwa die Art der Daten, die Eingriffsintensität und der Zeitpunkt.⁴ Eine Freiwilligkeit wird eher angenommen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Vor Abschluss des Arbeitsvertrags gelten zudem strengere Maßstäbe, da die Drucksituation für Bewerber größer ist als für bestehende Beschäftigte.⁵ Die beschriebenen Anforderungen gelten auch für die Verarbeitung besonderer Kategorien personenbezogener Daten, sofern sich die Einwilligung ausdrücklich auf diese Daten bezieht.

3 EuGH Urte. v. 30.03.2023, C-34/21, Rn. 65, 71, 74, 81 f. – diese Entscheidung betrifft das § 23 Abs. 1 S. 1 HDSIG. Auch das BAG nimmt eine Unanwendbarkeit des wortgleichen § 26 Abs. 1 S. 1 BDSG an, BAG Urte. v. 08.05.25, 8-AZR 209/21, Rn. 16.

4 Gola/Heckmann/Gola/Pötters, 3. Aufl. 2022, § 26 BDSG, Rn. 68; Kramer IT-ArbR/Oberthür, 3. Aufl. 2023, § 2 BDSG, Rn. 497.

5 Franzen, ErFK, 25. Aufl. 2025, § 26 BDSG, Rn. 41.

1.1.3 Die automatisierte Entscheidung nach Art. 22 DSGVO

KI-Verarbeitungen sind in der Praxis regelmäßig zudem an Art. 22 DSGVO zu messen. Danach darf niemand einer ausschließlich automatisierten Entscheidung, einschließlich Profiling, unterworfen werden, die rechtliche Wirkung entfaltet oder erheblich beeinträchtigt. Profiling umfasst *jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten*, Art. 4 Nr. 4 DSGVO. Es handelt sich damit um eine Form der Datenverarbeitung, die stets auf die Bewertung oder Prognose individueller Merkmale gerichtet ist und eine besondere Eingriffsintensität in die Rechte und Freiheiten der betroffenen Person aufweist.

Zulässig sind solche automatisierten Entscheidungen nur mit ausdrücklicher Einwilligung oder wenn sie für den Vertragsabschluss oder die Vertragserfüllung erforderlich sind (Art. 22 Abs. 2 DSGVO). Selbst dann muss der Verantwortliche nach Art. 22 Abs. 3 DSGVO sicherstellen, dass geeignete Maßnahmen zum Schutz der Rechte, Freiheiten und berechtigten Interessen der betroffenen Person getroffen werden.

1.1.4 Informationspflichten der DSGVO

Der Einsatz von KI-Systemen verlangt von Arbeitgebern ein hohes Maß an Transparenz und eine umfassende Information der betroffenen Personen. Unternehmen müssen besonders darauf achten, alle notwendigen Informationen zu erhalten, um den Informationspflichten nach Art. 13, 14 DSGVO gerecht zu werden. Dabei müssen sie auch über die Funktionsweise der KI, deren Entscheidungslogik sowie über die möglichen Folgen für die betroffenen Beschäftigten verständlich informieren.⁶ Alle Betroffenen müssen nachvollziehen können, wie ihre Daten im Zusammenhang verarbeitet werden und wie sie ihre Rechte wirksam ausüben können.

Gerade der Einsatz von KI-Systemen führt häufig dazu, dass automatisierte Entscheidungen oder Profiling vorgenommen werden. Besonders herausfordernd ist in der Praxis die klare und verständliche Offenlegung, ob und wie solche Verfahren eingesetzt werden (Art. 13 Abs. 2 lit. f) DSGVO). Die Unterstützung bei der Erfüllung der Informationspflichten sollte daher bereits bei der Dienstleistungsauswahl berücksichtigt werden.

6 Vgl. dazu Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024.

1.1.5 Betroffenenrechte der DSGVO

Die DSGVO stattet Betroffene in den Art. 15 bis 22 DSGVO mit weitreichenden Betroffenenrechten aus. Besonders praxisrelevant sind das Recht auf Auskunft nach Art. 15 DSGVO sowie das Recht auf Löschung der personenbezogenen Daten (sog. *Recht auf Vergessenwerden*) nach Art. 17 DSGVO. Das Auskunftsrecht begründet einen Anspruch darauf zu erfahren, zu welchen Zwecken ihre Daten verarbeitet werden, welchen Umfang die Verarbeitung hat, an welche Empfänger die Daten gelangen und wie lange eine Speicherung vorgesehen ist. Zudem haben Betroffene das Recht, keiner automatisierten Entscheidung nach Art. 22 DSGVO unterworfen zu werden.

Besondere Praxisherausforderungen ergeben sich für die Betroffenenrechte sowie für die Informationspflichten **betreffs** der Möglichkeit eines vollständigen Verständnisses des KI-Systems sowie der Möglichkeiten zur Datenextraktion und vollständigen Löschung.⁷

1.2 Die KI-Verordnung

Während die DSGVO den allgemeinen Rahmen für den Datenschutz vorgibt, regelt die KI-VO spezifisch den Einsatz von KI-Systemen. Art. 3 Nr. 1 KI-VO definiert ein „KI-System“ als ein maschinengestütztes System, das für einen in unterschiedlichem Grad autonomen Betrieb ausgelegt ist, nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben explizite oder implizite Ziele ableitet. Mit Hilfe eines KI-Systems können Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.

Adressaten der KI-VO sind insbesondere Anbieter und Betreiber des KI-Systems. Für den Umfang der Pflichten aus der KI-VO ist die jeweilige Rollenzuweisung ausschlaggebend. Im Personalwesen wird es meist auf die Unterscheidung zwischen Anbieter oder Betreiber ankommen. Anbieter ist, wer eine wesentliche Rolle bei der Entwicklung eines KI-Systems spielt oder es in ein eigenes Produkt übernimmt und dieses unter dem eigenen Namen auf den Markt bringt. Demgegenüber ist Betreiber, wer ein KI-System in eigener Verantwortung lediglich verwendet. In der Praxis ergibt sich kein starrer Übergang zwischen der Rolle als Anbieter und Betreiber – es ist daher stets eine Prüfung im Einzelfall erforderlich. Unter bestimmten Umständen kann ein Betreiber in die Rolle eines Anbieters wechseln, etwa wenn er wesentliche Änderungen an der Funktionali-

tät eines KI-Systems vornimmt (Stichwort *Customizing*) oder dieses unter eigenem Namen weiterverbreitet.

Nach Beleuchtung der Risikoeinordnung erfolgt eine kurze Darstellung der wesentlichen Pflichten nach der KI-Verordnung. Ein wesentlicher Teil der praxisrelevanten Pflichten ergibt sich dabei für Hochrisiko KI-Systeme. Nicht näher beleuchtet werden im Folgenden die Pflichten für Anbieter von KI-Systemen für einen allgemeinen Verwendungszweck (kurz GPAI).

1.2.1 Hochrisiko oder nicht?

Die KI-Systeme werden nach einem risikobasierten Ansatz in unterschiedliche Risikoklassen unterteilt: verbotene Praktiken, Hochrisiko KI-Systeme, Systeme mit begrenztem Risiko und solche mit keinem oder minimalem Risiko.⁸ Der Art. 6 der KI-VO legt für die Einordnung als Hochrisiko KI-System Kriterien fest und verweist auf Anhang III der Verordnung. Danach sind verschiedene KI-Systeme aufgeführt, die grundsätzlich als Hochrisiko KI-System einzustufen sind. Dort findet sich auch die Kategorie „Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit“. Dazu gehören KI-Systeme, die bei der Einstellung oder Auswahl von Personen eingesetzt werden, etwa zur Schaltung von Stellenanzeigen, zur Vorauswahl von Bewerbungen oder zur Bewertung von Kandidaten. Erfasst sind auch KI-Systeme, die Arbeitsbedingungen, Beförderungen oder Kündigungen beeinflussen, Aufgaben nach individuellen Merkmalen zuteilen oder die Leistung und das Verhalten von Beschäftigten überwachen.

Abweichend von der grundsätzlichen Einstufung findet sich in Art. 6 Abs. 3 KI-VO eine Rückausnahme als Einstufung als Hochrisiko KI-System: Danach kann ein in Anhang III genanntes KI-System im Einzelfall ausnahmsweise nicht als Hochrisiko KI-System gelten, wenn es kein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte mit sich bringt und das Entscheidungsergebnis nicht maßgeblich beeinflusst. Das gilt insbesondere dann, wenn das System nur eine eng begrenzte technische Aufgabe übernimmt, menschliche Arbeitsergebnisse unterstützt oder lediglich Muster erkennt, ohne eine abgeschlossene menschliche Bewertung zu ersetzen. Ein Beispiel ist eine KI, die Bewerbungsunterlagen nur nach formalen Kriterien wie Noten vorsortiert, ohne eine eigene Bewertung vorzunehmen. Solche KI-Systeme übernehmen lediglich eine eng begrenzte Hilfsfunktion, sodass kein zusätzliches Risiko für die Grundrechte der Bewerber entsteht. In einem solchen Fall spricht vieles für die Anwendung der Rückausnahme nach Art. 6 Abs. 3 KI-VO. Allerdings

⁷ Vgl. Paal/Kaulartz/Braegelman AI und Machine Learning-HdB, 1. Aufl. 2020, Kap. 8.7, Rn. 7.

⁸ Gerlach/Straßer, AI-Tools als Arbeitsmittel im betrieblichen Alltag – Chancen und Risiken für Arbeitnehmer und Arbeitgeber, ArbRAktuell 2024, 473, 475.

greift die Ausnahme nicht, wenn das KI-System ein Profiling vornimmt – dann bleibt es stets bei der Einstufung als Hochrisiko KI-System.

1.2.2 Pflichten für Hochrisiko KI-Systeme

Die Pflichten für Hochrisiko-KI-Systeme nach der KI-VO unterscheiden sich nach der Anbieter- und Betreiberrolle – die folgende Darstellung dient daher nur einem ersten Überblick:

Auch die KI-VO sieht Transparenzpflichten vor – diese stehen neben den Pflichten aus der DSGVO. Art. 26 KI-VO regelt die besonderen Transparenz- und Informationspflichten für Betreiber von Hochrisiko KI-Systemen, insbesondere dann, wenn diese im Zusammenhang mit Entscheidungen über natürliche Personen eingesetzt werden. Damit soll unter anderem sichergestellt werden, dass wesentliche Entscheidungsfaktoren nachvollziehbar bleiben.

Weitere Pflichten betreffen u. a. ein Risikomanagementsystem (siehe Art. 9 KI-VO), technische Dokumentationspflichten und Aufzeichnungspflichten (siehe Art. 11, 12 KI-VO), eine menschliche Aufsicht (siehe Art. 14 KI-VO), technische Schutzmaßnahmen betreffend die Genauigkeit, Robustheit und Cybersicherheit (siehe Art. 15 KI-VO) sowie die Durchführung einer Grundrechte-Folgenabschätzung (siehe Art. 27 KI-VO) – diese kann in der Praxis an die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO anknüpfen.

2 Von der Theorie in die Praxis: Praktisch relevante Use Cases

KI bietet zahlreiche Anwendungsmöglichkeiten im Personalwesen, von der Bewerberauswahl bis zur Personalentwicklung. Dabei ergeben sich vielfältige Chancen zur Effizienzsteigerung. Gleichzeitig müssen Unternehmen jedoch sicherstellen, dass datenschutzrechtliche Regelungen wie die DSGVO und die KI-VO eingehalten werden.

2.1 Automatisiertes Screening von Bewerbungen

KI-gestützte Tools können unter anderem Lebensläufe und Anschreiben nach Qualifikationen durchsuchen und Bewerbungen automatisch vorsortieren.

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten im Bewerbungsverfahren stützt sich regelmäßig darauf, dass diese für die Anbahnung oder Durchführung eines Beschäftigungsverhältnisses erforderlich ist.⁹ Das Sichten und Bewerten der Bewerbungs-

⁹ Vgl. HmbBfDI, Bewerberdatenschutz im Recruiting im Fokus; Hersemeyer/Ludolph, DSRITB 2023, 365.

unterlagen zählt zu den Maßnahmen, die auf ein späteres Beschäftigungsverhältnis abzielen. Grundsätzlich ebenso denkbar ist eine Einwilligung, deren Freiwilligkeit jedoch besonders kritisch zu prüfen ist. Die Freiwilligkeit fehlt beispielsweise dann, wenn diese an eine Vertragschance geknüpft wird.¹⁰ Für die Abgrenzung zwischen der Erforderlichkeit zur Vertragserfüllung und der Einwilligung ist in der Praxis stets das Merkmal der *Erforderlichkeit* in den Fokus zu rücken – ohne Einwilligung sind nur solche Verarbeitungen möglich, die im konkreten Fall als erforderlich zu qualifizieren sind. Nötig bleibt daher eine Betrachtung im Einzelfall. Neben der Rechtmäßigkeit der Verarbeitung ist die Zweckbindung zu berücksichtigen: Es muss sichergestellt werden, dass die Daten nicht für weitere Zwecke verarbeitet werden.¹¹

Wenn ein KI-System selbstständig darüber entscheidet, ob eine Bewerbung weiter berücksichtigt wird oder nicht, etwa indem Bewerber anhand eines Punktesystems automatisch abgelehnt werden, kann das erhebliche Folgen für die Betroffenen haben.¹² Der EuGH entschied, dass bereits eine automatisierte Handlung, die den Entscheidungsprozess „maßgeblich prägt“, als „ausschließlich automatisierte“ Entscheidung gelten kann.¹³ Dies bedeutet, dass zudem die Anforderungen des Art. 22 DSGVO zu berücksichtigen sind, wenn zwar offiziell ein Mensch beteiligt ist, dieser aber in der Praxis die von der KI getroffene Entscheidung lediglich ungeprüft übernimmt. Entscheidend ist folglich, dass das Screening lediglich als Vorbereitungsmaßnahme gesehen wird und eine echte menschliche Aufsicht die finale Entscheidung unter Berücksichtigung aller relevanten Faktoren übernimmt.¹⁴

KI-Systeme zum Screening und Bewerten von Bewerbungen können unter Berücksichtigung von Art. 6 Abs. 2 i. V. m. Anhang III Nr. 4 lit. a) KI-VO als Hochrisiko KI-Systeme einzustufen sein.¹⁵ Davon erfasst sind KI-Systeme, die bei der Einstellung oder Auswahl von Personen eingesetzt werden, zum Beispiel für gezielte Stellenanzeigen, das Sichten oder Filtern von Bewerbungen oder die Bewertung von Bewerbern.¹⁶ Art. 6 Abs. 3

¹⁰ Laut ErWG 43 S. 2 DSGVO ist eine Einwilligung nicht freiwillig, wenn die Erfüllung eines Vertrags von der Einwilligung abhängt, obwohl diese für die Vertragsdurchführung nicht erforderlich ist

¹¹ Vgl. Kindshofer, ZD 2024, 673, 675.

¹² ErWG 71 S. 1 DSGVO sagt, dass „Online-Einstellungsverfahren ohne jegliches menschliches Eingreifen“ als ein Beispiel für rechtlich wirkende oder in ähnlicher Weise erheblich beeinträchtigende Entscheidungen im Sinne des Art. 22 Abs. 1 DSGVO darstellt.

¹³ EuGH Ur. v. 07.12.2023 – C-634/21: Zur Auslegung des Begriffs „automatisierte Entscheidung im Einzelfall“ i. S. d. Art. 22 Abs. 1 DSGVO („SCHUFA Holding“).

¹⁴ Kätcher/Pesch, KIR 2024, 26; Gerlach/Straßer, ArbRAktuell 2024, 473.

¹⁵ Frank/Heine, Die algorithmische Personalauswahl, CB 2024, 326, 328.

¹⁶ Vgl. Frank/Heine, CB 2024, 326.

S. 1 der KI-VO sieht jedoch bestimmte Ausnahmeregelungen vor. Eine solche Ausnahme ist vorliegend insbesondere dann möglich, wenn die KI-Systeme lediglich vorbereitende Aufgaben erledigen. Eine der entscheidenden Voraussetzungen für eine Ausnahme ist, dass kein Profiling stattfindet.¹⁷ Kein Hochrisiko-KI-System liegt folglich vor, wenn das Screening lediglich als Vorbereitungsmaßnahme genutzt wird und eine echte menschliche Aufsicht die finale Entscheidung unter Berücksichtigung aller relevanten Faktoren übernimmt.¹⁸

Zu beachten ist stets das Risiko von Bias. Damit sind Verzerrungen gemeint, die durch Daten oder Algorithmen entstehen und zu diskriminierenden Ergebnissen führen können.¹⁹ Enthalten Trainingsdaten etwa überwiegend Bewerbungen männlicher Führungskräfte, kann das KI-System weibliche Kandidatinnen benachteiligen.²⁰ Solche Effekte können einen Verstoß gegen das Allgemeine Gleichbehandlungsgesetz darstellen.²¹

2.2 Onboarding-Prozesse

Der Einstieg ins Unternehmen ist für neue Mitarbeitende ein wichtiger Moment. Zunehmend werden KI-gestützte Tools wie Chatbots, interaktive FAQs und smarte Lernpfade genutzt, um den Onboarding-Prozess zu standardisieren und individuell anzupassen.

Die Verarbeitung personenbezogener Daten kann auf Art. 6 Abs. 1 S. 1 lit. b) DSGVO gestützt werden, wenn sie zur Erfüllung des Beschäftigungsverhältnisses erforderlich ist. Zum anderen kann die Datenverarbeitung jedenfalls nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO zur Wahrung berechtigter Interessen des Arbeitgebers gerechtfertigt werden. In diesem Zusammenhang ist auch relevant, ob die betroffene Person aufgrund der Art ihrer Beziehung zum Arbeitgeber davon ausgehen konnte, dass ihre Daten verarbeitet werden.²² Ein Beschäftigter, der beispielsweise mit einem als Chatbot gekennzeichneten KI-System interagiert, wird in der Regel davon ausgehen, dass die eingegebenen Daten von der KI verarbeitet werden. In diesem Fall ist eine solche Verarbeitung rechtlich zulässig.²³

¹⁷ Lommatzsch/Albrecht, Einsatz von KI im Personalwesen von Unternehmen – Neue Herangehensweise nach Geltung der KI-VO, GWR 2025, 37, 38.

¹⁸ Kätscher/Pesch, KIR 2024, 26.

¹⁹ Im ErWG 57 wird dann noch weitergehend erläutert, dass insbesondere die Gefahr der Diskriminierung und der Fortschreibung von Diskriminierungsmustern droht, z.B. angesichts des Geschlechts oder der Religionszugehörigkeit; G.Kania in Küttner Personalbuch 2025, 32. Aufl. 2025, Künstliche Intelligenz, Rn. 5.

²⁰ Vgl. <https://www.reuters.com/article/world/insight-amazon-scrapsecret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MKOAG/>, abgerufen am 14.10.2025.

²¹ Löser, Nutzung von KI-Systemen im Bewerbungsprozess, öAT 2025, 70.

²² Dies ergibt sich auch aus ErWG 47 DSGVO.

²³ Golland, EuZW 2024, 846.

Solange diese KI-Systeme lediglich Informationen bereitstellen und organisatorische Unterstützung bieten, ergeben sich geringe Auswirkungen auf die Betroffenen.²⁴ Analysieren sie jedoch Verhaltensweisen oder Lernfortschritte, um Aussagen über Arbeitsstil, Eignung oder Leistung zu treffen, handelt es sich in der Regel um Profiling nach DSGVO. Solche Anwendungen unterliegen dann strengen datenschutzrechtlichen Vorgaben und können im Einzelfall als Hochrisiko KI-Systeme nach der KI-VO eingestuft werden. Dies gilt insbesondere dann, wenn die Systeme innerhalb des Onboardings u. a. zur Bewertung individueller Kompetenzen, Arbeitsleistung oder Verhaltensmuster eingesetzt werden – etwa um Rückschlüsse auf Entwicklungspotenziale der Beschäftigten zu ziehen. Bei Verwendung solcher Systeme werden Entscheidungen durch eine KI getroffen, welche die Bedingungen von u. a. Arbeitsverhältnissen oder Beförderungen beeinflussen können. Es besteht daher ein erhebliches Risiko einer Grundrechtsbeeinträchtigung.²⁵

2.3 Personalplanung

KI wird auch in der strategischen Personalplanung eingesetzt, um große Datenmengen zu analysieren und Prognosen zu erstellen. Sie wertet historische Daten zu Fluktuation, Überstunden und Krankheitsständen aus, erkennt Engpässe und identifiziert Weiterbildungsbedarf.

Bei einer Verarbeitung personenbezogener Daten im Rahmen der Personalplanung ist die Erforderlichkeit nach Art. 6 Abs. 1 S. 1 lit. b) DSGVO regelmäßig nicht gegeben, da die Auswertungen und Prognosen meist nicht zur Durchführung des Beschäftigungsverhältnisses erforderlich sind. Soweit die Grenze betreffend die Erforderlichkeit der Datenverarbeitung überschritten wird, bleibt insbesondere die Möglichkeit zur Einholung einer Einwilligung – dabei ist ein strenger Freiwilligkeitsmaßstab anzulegen. Sofern im Zusammenhang der Personalplanung auch besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO verarbeitet werden sollen (z. B. Gesundheitsdaten), ist die Einholung einer Einwilligung zwingend.

KI-Systeme die nur aggregierte Daten für allgemeine Prognosen nutzen und keine individuellen Entscheidungen treffen, gelten in der Regel nicht als Hochrisiko KI-Systeme. Solche KI-Systeme gelten nach Art. 6 Abs. 3 S. 1 KI-VO nicht als hochriskant, da sie anonymisierte Daten verarbeiten, um allgemeine strategische Prognosen zu erstellen. Hierbei besteht nicht die Möglichkeit, dass Rückschlüsse auf einzelne Personen oder individu-

²⁴ Vgl. Frank/Heine, CB 2024, 326.

²⁵ Koreng/Lachenmann, DatenschutzR-FormHdB/Lachenmann, 4. Aufl. 2025, Form. Q. II. Anm. 1.-5.

elle Maßnahmen getroffen werden können.²⁶ Hochrisiko-Anforderungen treten erst auf, wenn das System konkrete Maßnahmen gegenüber Einzelpersonen ergreift oder individuelle Bewertungen vornimmt. Dies ist der Fall, wenn Systeme zur Bewertung oder Beobachtung von Verhalten oder Leistungen einer Person eingesetzt werden, die das künftige Arbeitsverhältnis beeinflussen.²⁷ Entscheidend ist dabei, dass durch das System nicht allgemeine Trends analysiert werden, sondern zu individuellen Arbeitsverhältnissen spezifische Aussagen getroffen werden

3 Exkurs: Mitbestimmung des Betriebsrates

Bei dem Einsatz von KI-Systemen im Personalwesen ist auch das kollektive Arbeitsrecht – insbesondere § 87 Abs. 1 Nr. 6 BetrVG – zu berücksichtigen. Danach hat der Betriebsrat bei der Einführung und Anwendung technischer Einrichtungen, die objektiv zur Überwachung der Arbeitnehmer bestimmt sind, mitzubestimmen. Das Mitbestimmungsrecht des Betriebsrats greift insbesondere dann, wenn KI-gestützte Systeme dazu geeignet sind, das Verhalten oder die Leistung von Arbeitnehmern zu überwachen oder zu bewerten. Darunter fallen beispielsweise KI-Tools zur automatisierten Leistungsbewertung, zur Steuerung von Arbeitszeit, zur Einteilung von Arbeitskräften oder zur Analyse des Kommunikationsverhaltens. Es empfiehlt sich daher in der Praxis die frühzeitige Einbindung des Betriebsrates.

4 Was Unternehmen jetzt tun sollten

Zunächst ein praktischer Hinweis: Für die Prüfung der rechtlichen Anforderungen ergibt sich folgender Praxishinweis: Um die rechtlichen Anforderungen vollständig zu erfassen, sind bei allen rechtlichen Bewertungen die folgenden Ebenen eines KI-Systems zu berücksichtigen:

1. Eingabeschicht (= Input-Daten),
2. Verborgene Schicht,
3. Ausgabeschicht (= Output-Daten).

Eine rechtmäßige Datenverarbeitung und Nutzung des KI-Systems müssen stets alle genannten Ebenen erfassen.

sen. Sofern zudem ein Training erfolgt, ist dieses gesondert in die rechtliche Bewertung einzubeziehen.²⁸

DSGVO und KI-VO bieten Unternehmen einen verbindlichen Rahmen. Frühzeitige Umsetzung schafft Rechtssicherheit und Vertrauen. Die Übergangsfristen der KI-VO²⁹ sollten genutzt werden, um Systeme zu prüfen, Risiken zu bewerten und Mitarbeitende zu schulen. Transparente Information, lückenlose Dokumentation und die Sicherstellung der Datenqualität sind dabei zentral. Zudem sollten Unternehmen den Betriebsrat einbinden und interne Leitlinien für den ethischen und rechtlichen Umgang mit KI entwickeln. So können Bußgelder, Schadensersatzforderungen oder Reputationsschäden vermieden werden.

Der Blick in die Zukunft zeigt, dass KI im HR-Management an Bedeutung gewinnen wird, indem sie Prozesse optimiert und datengestützte Entscheidungen ermöglicht. Sie sollte jedoch unterstützend und nicht ersetzend wirken. Unternehmen, die früh auf Transparenz, klare Prozesse und ethische Leitlinien setzen, stärken ihre Arbeitgebermarke und sichern sich Zukunftsfähigkeit.



Dr. Patrick Grosmann, M.A. ist Rechtsanwalt bei FPS Rechtsanwälten in Frankfurt. Er ist zertifizierter Datenschutzbeauftragter (TÜV®) sowie zertifizierter Datenschutz-Auditor (DGI®) und berät Unternehmen in allen Fragen des Datenschutzes, des IT-Sicherheitsrechts und der KI-Nutzung.



Vivien Lauren Wale ist Rechtsreferendarin bei der Kanzlei FPS in Frankfurt im IT- und Datenschutz-Team sowie am Landgericht Frankfurt.

²⁶ Vgl. Schild/BeckOK DatenschutzR, 53. Ed., St. 01.08.2025, DA Art. 2, Rn. 31, 34

²⁷ Koreng/Lachenmann, DatenschutzR-FormHdB/Lachenmann, 4. Aufl. 2025, Form. Q. II. Anm. 1.-5.

²⁸ Vgl. zur Verarbeitung von Trainingsdaten, Reichert/Radtke/Eske, ZD 2024, 483, 484. Vgl. zu den Anforderungen der KI-VO: Dregelies, GRUR 2024, 1484.

²⁹ Siehe <https://artificialintelligenceact.eu/de/implementation-timeline/>, abgerufen am 14.10.2025.