



Die Nutzung von KI im Personalwesen: Orientierung im Dschungel der KI Regulierung

Vorstellung & Agenda

Referent:innen



Anna M. Bock

Rechtsanwältin, Fachanwältin für Arbeitsrecht / Senior Associate
Employment Law & Benefits
Deloitte Legal
Hannover, Germany

Tel.: +49 511 307559315
E-Mail: abock@deloitte.de



Roland Schiller

Rechtsanwalt / Associate
Digital Law
Deloitte Legal
Frankfurt am Main, Germany

Tel.: +49 69 71918 8473
E-Mail: rschiller@deloitte.de

Agenda

- I. Verordnung über künstliche Intelligenz
- II. Arbeitsrecht: Mitbestimmung bei der Einführung von KI
- III. Datenschutzrecht: Grundsätze und Bedeutung für KI
- IV. Use Case: Personalmaßnahmen
- V. KI-Governance
- VI. Exkurs: Entwurf des Beschäftigtendatengesetz (BeschDG)
- VII. Q & A



Verordnung über künstliche Intelligenz Verordnung (EU) 2024/1689

Die EU KI-Verordnung im Überblick

1

Handelt es sich um ein KI-System im Sinne von Art. 3 Abs. 1 KI-VO?

Ein „KI-System“ ist ein maschinengestütztes System, das für einen in wechselndem Maße autonomen Betrieb ausgelegt ist, 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.

2

In welche Risikokategorie fällt das KI-System?

Verbotenes KI-System

Hochrisiko-KI-System

Begrenztes Risiko

Minimales Risiko

3

Um welche Art von „Akteur“ handelt es sich?

Anbieter

Betreiber

Einführer

Händler

Hersteller

Bevollm. Vertreter

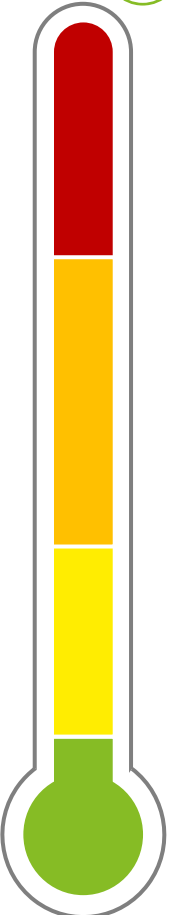
4

Handelt es sich bei dem KI-System um eine General Purpose AI (GPAI)?

GPAI „normal“

GPAI mit systemischem Risiko ($> 10^{25}$ FLOPS)

Förderung menschenzentrierter und vertrauenswürdiger KI zum Schutz von Gesundheit, Grundrechten, Demokratie und Umwelt – bei gleichzeitiger Unterstützung von Innovationen und europäischen KMUs

!	Risikokategorie	>>	Konsequenz	🕒	Umsetzungsfrist	💰	Bußgelder bis zu ...
	Unannehmbares Risiko <ul style="list-style-type: none"> • Soziales Scoring • Biometrische Identifizierung in Echtzeit • Emotionen am Arbeitsplatz wahrnehmen ^{a)} 	➔	Verbote	➔	6 Monate	35 Mio. € oder 7% des weltweiten Jahresumsatzes <ul style="list-style-type: none"> • Unannehmbare Anwendungsfälle (Art. 5) 	
	Hochrisiko-KI-Systeme <ul style="list-style-type: none"> • Kreditentscheidung • Kritische Infrastruktur • Risiko für Grundrechte • Die in Anhang III aufgeführten Sonderfälle 	➔	Konformitätsprüfung, Governance, Überwachung, Protokollierung	➔	24 bis 36 Monate ^{b)} 12 Monate (GPAI-Systeme)	15 Mio. € oder 3% des weltweiten Jahresumsatzes <ul style="list-style-type: none"> • Nichteinhaltung der Betreiberpflichten bei Hochrisiko-KI-Systemen 	
	Begrenztes Risiko <ul style="list-style-type: none"> • Chatbots • „Deep Fakes“ 	➔	Transparenzverpflichtungen	➔	24 Monate	7,5 Mio. € oder 1% des weltweiten Jahresumsatzes <ul style="list-style-type: none"> • Falsche, unvollständige oder irreführende Antwort auf eine Anfrage der NZB/NB^{c)} 	
	Minimales Risiko/sonstiges Risiko <ul style="list-style-type: none"> • Interne Modelle • Verfahrenstechnische Aufgaben 	➔	Freiwillige Standards	➔	n.a.		

^{a)} Außer bei Müdigkeit oder Schmerzen.; ^{b)} Bis zu 36 Monate, wenn der Anwendungsfall in der EU-Produktsicherheitsliste aufgeführt ist.; ^{c)} NZB = nationale zuständige Behörde, NB = notifizierende Behörde. Produkte, die bereits vor der KI-Verordnung auf dem Markt waren, werden technisch vom Anwendungsbereich ausgenommen, es sei denn, sie sind bereits auf dem Markt und (i) erfahren danach „signifikante Veränderungen“ oder (ii) sind eine GPAI. Außerdem gilt für GPAI, die bereits vor der KI-Verordnung auf dem Markt waren, eine verlängerte Umsetzungsfrist von 36 Monaten.

Beispiele für den Einsatz von KI im HR-Bereich und zur Umsetzung der Arbeit



Hochrisikosysteme gem. Anhang III

[...]

Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit:

a) **Einstellung oder Auswahl** natürlicher Personen, insbesondere gezielte Stellenanzeigen, Sichten, Filtern Bewerten von Bewerbungen / Bewerbern

b) **Entscheidungen**, die die Bedingungen von Arbeitsverhältnissen, Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen beeinflussen;

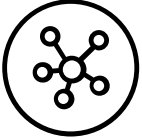
Zuweisung von Aufgaben aufgrund des individuellen Verhaltens oder persönlicher Merkmale oder Eigenschaften; **Beobachtung und Bewertung** der Leistung und des Verhaltens von Personen



Ausnahme: kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen, indem KI-System unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst.

Pflichten des Betreibers*


„Betreiber“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet




Technische und organisatorische Maßnahmen sicherstellen




Durchführung einer DSFA




Aufbewahrung von KI-generierten Protokollen




Menschliche Aufsicht




Betroffeneninformation und Recht auf Erläuterung der Entscheidungsfindung im Einzelfall




KI-Nutzungskompetenz sicherstellen



Informationspflichten vor der Inbetriebnahme am Arbeitsplatz



Ggf. Registrierungspflicht der KI (Organe, Einrichtungen oder sonstige Stellen der Union)



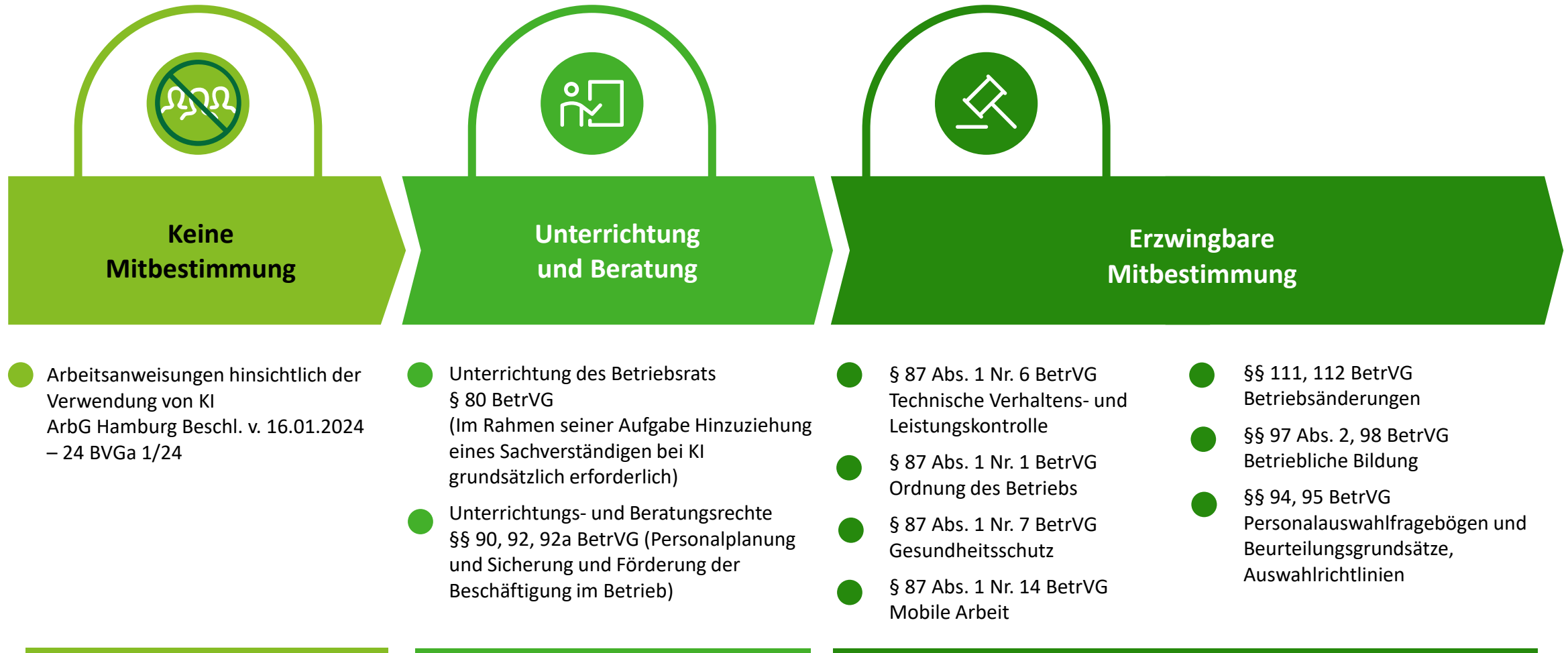
Überwachung des Betrieb, inkl. der Eingabedaten von KI; Melde- und Informationspflichten

*) Die dargestellten Pflichten des Betreibers entsprechen den „Pflichten der Betreiber von Hochrisiko-KI-Systemen“ nach Art. 26 KI-Verordnung.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat eine Orientierungshilfe zu „Künstliche Intelligenz und Datenschutz“ herausgegeben (Version 2.0 vom 17. Oktober 2024), die den Einsatz von KI-Systemen durch Verantwortliche aus datenschutzrechtlicher Sicht beleuchtet.

Arbeitsrecht: Mitbestimmung bei der Einführung von KI

Wesentliche Mitbestimmungsrechte des Betriebsrates bei der Einführung von KI



Mitbestimmung des Betriebsrates bei der Einführung von KI

Unterrichtung und Beratung

- Betriebsrat muss nicht zustimmen
- Einigungsstelle kann grundsätzlich nicht angerufen werden
- Der Arbeitgeber muss den Betriebsrat unterrichten und mit dem Betriebsrat beraten und sich ernsthaft damit befassen. Lehnt er die Vorschläge ab, muss er das ggf. (schriftlich) begründen
- Bei Verletzung kann Erfüllungsanspruch im Beschlussverfahren durchgesetzt werden und nach § 23 Abs. 3 BetrVG mit einem Ordnungsgeld sanktioniert werden

Erzwingbare Mitbestimmung

- Betriebsrat muss zwingend zustimmen
→ Betriebsvereinbarung
- Einigungsstelle wird auf Antrag einer Partei tätig
→ Spruch der Einigungsstelle ersetzt die Einigung mit dem Betriebsrat
- Beseitigungs- und Unterlassungsanspruch
→ Besteht bei Verletzung der Mitbestimmungsrechte aus § 87 Abs. 1 BetrVG
→ Durchsetzung gerichtlich, auch per einstweiliger Verfügung, möglich

Mitbestimmung bei der Umsetzung der Arbeitgeberpflichten aus der KI-VO



Arbeitnehmerinformation

- Vor Inbetriebnahme oder Verwendung eines Hochrisiko-KI-Systems am Arbeitsplatz müssen die Betreiber, die Arbeitgeber sind, die Arbeitnehmervertreter und die betroffenen Arbeitnehmer darüber informieren, dass sie Gegenstand des Einsatzes des Hochrisiko-KI-Systems sein werden (Art. 26 Abs. 7 KI-VO)



Ergänzung von Policies, Handbüchern

- Umsetzung der Vorgaben der KI-Verordnung durch entsprechende Ergänzung von Policies, Handbüchern: Ggf. Mitbestimmung aus § 87 Abs. 1 Nr. 1 BetrVG



KI-Kompetenz-Schulungen Art. 4 KI-VO

- Einführung und Umsetzung von KI-Kompetenzschulungen: Mitbestimmung nach §§ 97, 98 BetrVG



Information über und Erläuterung der Entscheidungsfindung

- Treffen Betreiber auf der Grundlage der Daten aus einem Hochrisiko-KI-System eine Entscheidung, die rechtliche Auswirkungen hat oder die von der Entscheidung betroffene Person in ähnlicher Art erheblich auf eine Weise beeinträchtigt, die ihrer Ansicht nach ihre Gesundheit, ihre Sicherheit oder ihre Grundrechte beeinträchtigt, hat die betroffene Person das Recht, vom Betreiber eine klare und aussagekräftige Erläuterung zur Rolle des KI-Systems im Entscheidungsprozess und zu den wichtigsten Elementen der getroffenen Entscheidung zu erhalten (Art. 86 KI-VO) und Information von Betroffenen (Art. 26 Abs. 7 KI-VO): Mitbestimmung des Betriebsrates nach § 87 Abs. 1 Nr. 1 oder Nr. 6 BetrVG

Best Practice

Ggf. Zusammenarbeit mit dem Betriebsrat bei Erstellung von KI-Grundsätzen



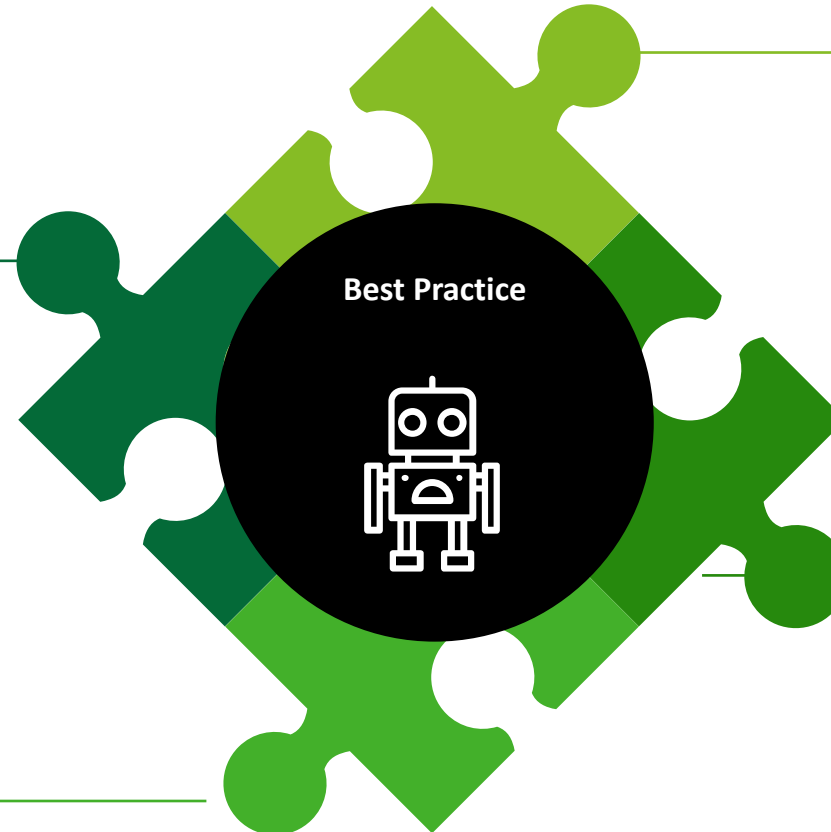
Interdisziplinär konsistent abgestimmte Implementierung des KI-Systems aus arbeitsrechtlicher, datenschutz- / IT-rechtlicher und technischer Sicht



Frühzeitige Beteiligung des Betriebsrats und verständliche Aufklärung auch über datenschutzrechtliche regulatorische und technische Aspekte bei der Implementierung des IT-Systems



Berücksichtigung der Betriebsvereinbarungsverhandlungen im Implementierungszeitplan



Datenschutzrecht

Grundsätze und Bedeutung für KI

KI und Datenschutz

Verhältnis zwischen KI-Verordnung und DSGVO



Die Grundrechte und Grundfreiheiten von betroffenen Personen müssen effektiv geschützt werden. Für die Entwicklung und den Einsatz von KI-Systemen, in denen personenbezogene Daten verarbeitet werden, sind daher neben der KI-Verordnung die Vorgaben der DSGVO zu beachten.

DSGVO

- Schutz personenbezogener Daten steht im Vordergrund
- DSGVO bleibt durch die KI-Verordnung unberührt
- Überprüfung der Datensätze nach Art. 10 KI-Verordnung ist bereits eine Verarbeitung personenbezogener Daten und muss auf einer Rechtsgrundlage nach Art. 6 DSGVO beruhen



KI-Verordnung

- Gibt Rahmen für den generellen Umgang mit Daten vor (Data-Governance)
- Zentrale Regulierungsvorschrift zu Datenverarbeitung: Art. 10 KI-Verordnung
- Sofern Hochrisiko-KI-Systeme mit Daten trainiert werden, müssen entsprechende Qualitätskriterien eingehalten werden



- Beide Verordnungen gelten **nebeneinander**
- Werden personenbezogene Daten bei der Entwicklung von Hochrisiko-KI-Systemen verwendet, müssen Anbieter sowohl die Vorgaben der KI-Verordnung, als auch die der DSGVO einhalten, sog. „**Doppelverpflichtung**“

Datenschutzrechtliche Grundsätze und Bedeutung für KI (Auswahl)

1*

Erhebung von Trainingsdaten

2

Verarbeitung von Trainingsdaten inkl. „Fine-Tunings“

3

Bereitstellung von KI Anwendungen

Nutzung von Eingabedaten zu Trainingszwecken

4

Nutzung von KI Anwendungen

5

Nutzung von Ergebnissen von KI Anwendungen



Zweckbindung

Es muss vorab festgelegt werden, welches Einsatzfeld für die KI vorgesehen ist. Ist die Verarbeitung personenbezogener Daten für die Erreichung des Zwecks erforderlich?



„Privacy by Design“ und „Privacy by Default“

z.B. Einschränkung der Verarbeitung von im Live-Betrieb eingegebenen personenbezogenen Daten für das KI-Training



„Integrität und Vertraulichkeit“

Insbesondere Schutz vor Model Inversion Attacks und Membership Inference Attacks



Datenminimierung

Beschränkung der Verarbeitung von personenbezogenen Daten auf das absolut Erforderliche



Datenrichtigkeit

Die verarbeiteten Daten müssen vorab auf ihre Richtigkeit geprüft werden. Eine nachträgliche Korrektur unrichtiger Daten muss effektiv möglich sein.

*) Fünf Phasen der Verarbeitung nach dem Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz der Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg (Version 2.0 vom 17.10.2024).

Use Case: Personalmaßnahmen

Bewerbermanagement



CV-Parsing

- Identifizierung von Schlüsselparametern
- Aussortieren von unpassenden Bewerbungen



Candidate Journey

- Nutzung eines Chatbots
- Erstellung von Persönlichkeitsprofilen durch die Analyse von Text und Sprache
- Auswertung von Sprache, Mimik und Gestik

Erwartete Vorteile

- Effizienter Einsatz von Ressourcen
- Kostensenkung
- Erhöhte Objektivität im Auswahlprozess (Bias-Reduktion) durch datenbasierte Entscheidungen anstatt subjektiven Eindrücken



Risiken

Insbesondere bei der Nutzung eines „falschen“ Datensatzes bestehen erhebliche Risiken der offenen/versteckten Diskriminierung:

- „voreingenommener“ Datensatz; Berücksichtigung diskriminierender Parameter wie Geschlecht oder Herkunft
- Überbewertung bestimmter Kriterien (bestimmte Key-Words werden häufiger von Männern oder Frauen verwendet)

Bewerbermanagement

KI-Verordnung (Auswahl)

- Liegt ein Hochrisiko-KI-System vor oder ist der Einsatz ausnahmsweise nicht mit einem hohen Risiko verbunden.
- KI Kompetenz der Beschäftigten muss sichergestellt werden.
- Arbeitnehmer und Betroffene müssen über die Verwendung eines KI-Systems informiert werden.
- Entscheidungen durch das KI-System müssen erklärbar sein.

Verbotene Praxis i.S.v.
Art. 5 KI-VO?



Datenschutz (Auswahl)

- Verarbeitung nur auf Basis einer Rechtsgrundlage; ist der Einsatz von KI erforderlich?
- Die Verarbeitung von besonderen Kategorien personenbezogener Daten (z.B. Stimme/Mimik) ist nur unter erweiterten Voraussetzungen zulässig.
- Besondere Herausforderungen stellen sich bei der Freiwilligkeit der Einwilligung im Über- Unterordnungsverhältnis.
- Menschliche Überwachung über Entscheidungen von KI muss sichergestellt sein (Art. 22 DSGVO).
- Durchführen einer Datenschutzfolgenabschätzung.
- Betroffenenrechte müssen effektiv umsetzbar sein.



Arbeitsrecht (Auswahl)

- Vor der Einführung des KI-Systems ist mit dem Betriebsrat idR eine Betriebsvereinbarung abzuschließen, § 87 Abs. 1 Nr. 6 BetrVG.
- Die Aufstellung von standardisierten Fragen und von Grundsätzen der Entscheidungsfindung im Bewerbungsprozess durch das KI-System unterliegen der Mitbestimmung nach § 95 BetrVG.
- Im Rahmen der Mitbestimmung bei personellen Einzelmaßnahmen nach § 99 BetrVG ist der Betriebsrat über den Einsatz und die Ergebnisse des KI-Systems bei der Bewerberauswahl zu informieren.



KI Governance

Umsetzung der KI-Verordnung

Überblick

Umsetzungsphase

- Umsetzung des Maßnahmenplans zur Implementierung der KI-Anwendungsfälle
- Schulung / Training der Mitarbeitenden
- Schaffung einer Compliance-by-Design-Kultur innerhalb des Unternehmens und Integration der neuen Compliance-Prozesse in bestehende (Privacy) Strukturen
- Anpassung der Compliance- und Ethik-Richtlinien anhand der Erfahrungen in der Praxis

Vorbereitungsphase

- KI-Readiness Assessment (Bestandsaufnahme von KI-Systemen und bereits bestehenden Compliance/Privacy-Strukturen)
- Definition von (weiteren) KI-Anwendungsfällen und Einordnung in Risiko- sowie Akteur-Klassen nach der KI-Verordnung
- Zusammenstellung der weiteren rechtlichen, ethischen und technischen Anforderungen und Entwicklung von internen Compliance- und Ethik-Richtlinien
- Entwicklung von Schulungs- und Trainingsmaterialien
- Erstellung eines klaren und zeitlich festgelegten Maßnahmenplans zur Umsetzung der Ziele
- Einbeziehung und Information des Betriebsrates, ggf. Aufnahme von Verhandlungen

Monitoring

- Fortlaufende Überwachung der regulatorischen und technischen Landschaften
- Fortlaufende Bewertung der KI-Anwendungsfälle und Anpassung der Risikoeinordnungen, Richtlinien, Anwendungsfälle etc.
- Etablierung eines Systems automatischer Kontrollen zur kontinuierlichen Überwachung neuer Software (z.B. Freigabe-Workflows)

Exkurs: Entwurf des Beschäftigtendatengesetz (BeschDG)

Referentenentwurf des Beschäftigtendatengesetz (BeschDG)

Bisher existieren kaum speziell auf den Schutz von Beschäftigtendaten zugeschnittene Regelungen. Mit dem BeschDG wird der Rahmen für einen modernen Beschäftigtendatenschutz geschaffen, der eine Balance zwischen den Interessen der Betriebe und der Beschäftigten zum Ziel hat und dabei gleichzeitig den erforderlichen Schutz für die Beschäftigten gewährleistet.

Kerninhalte



- **Transparente und klare Regelungen** für Beschäftigtendaten
- Datensicherheit durch **Technische und organisatorische Maßnahmen**
- **Verwertungsverbot** datenschutzwidrig verarbeiteter Daten
- **Strenge Vorgaben** für die automatisierte Datenverarbeitung

Rechte und Pflichten des Arbeitnehmers



- Kollektivvereinbarungen scheiden als datenschutzrechtliche Rechtsgrundlage für eine Verarbeitung aus.
- Konkretisierung einer wirksamen **Einwilligung** in die Verarbeitung von Beschäftigtendaten Freie Widerrufbarkeit
- **Recht auf Information** über Datenverarbeitung und Ergebnis

KI-Regulierung




- **Transparenzpflichten/Betroffenenrechte** für den Einsatz von KI
- **Monitoring** der Erforderlichkeit von Verarbeitungen und unrichtige Ergebnisse als **Technische und organisatorische Maßnahme**

💡 Outlook



Das Beschäftigtendatengesetz stärkt den Datenschutz am Arbeitsplatz und schafft klare Rahmenbedingungen im Umgang mit Beschäftigtendaten. Zukünftige Entwicklungen im Bereich der Digitalisierung werden jedoch kontinuierliche Anpassungen der Regelungen erfordern, um den Schutz der Arbeitnehmerrechte zu gewährleisten.

III. Q&A



Vielen Dank
für Ihre
Aufmerksamkeit

Deloitte Legal

Ihr Kontakt



Anna M. Bock
Rechtsanwältin, Fachanwältin für Arbeitsrecht / Senior
Associate
Employment Law & Benefits
Deloitte Legal
Hannover, Germany

Tel.: +49 511 307559315
E-Mail: abock@deloitte.de



Roland Schiller
Rechtsanwalt / Associate
Digital Law
Deloitte Legal
Frankfurt am Main, Germany

Tel.: +49 69 71918 8473
E-Mail: rschiller@deloitte.de

Where legal meets business

Deloitte Legal, das sind

mehr als **2.500** Rechtsanwälte
in **75+** Ländern



die eng zusammenarbeiten
über nationale Grenzen hinweg und
gemeinsam mit anderen Deloitte-
Geschäftsbereichen

Services von Deloitte Legal

Unsere drei sich überschneidenden Servicebereiche ermöglichen es uns, unsere Mandanten wann und wo benötigt und in der jeweils optimal geeigneten Form bei der Realisierung ihrer Visionen zu beraten.



Wir schaffen (Mehr)Werte

Als Teil des weltweiten Deloitte-Netzwerks arbeitet Deloitte Legal mit einer Vielzahl anderer Fachrichtungen zusammen und bietet multinationale juristische Lösungen und weltweit integrierten Service:



in Einklang

mit Ihrer unternehmensweiten Vision



maßgeschneidert

für Ihre Geschäftsbereiche und Niederlassungen



technologiestützt

für verbesserte Zusammenarbeit und Transparenz



abgestimmt

auf Ihre regulatorischen Anforderungen



Deloitte Legal bezieht sich auf die Rechtsberatungspraxen der Mitgliedsunternehmen von Deloitte Touche Tohmatsu Limited, deren verbundene Unternehmen oder Partnerfirmen, die Rechtsdienstleistungen erbringen.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen des Einzelfalls gerecht zu werden und ist nicht dazu bestimmt, Grundlage für wirtschaftliche oder sonstige Entscheidungen zu sein. Weder die Deloitte Legal Rechtsanwalts-gesellschaft mbH noch Deloitte Touche Tohmatsu Limited, noch ihre Mitgliedsunternehmen oder deren verbundene Unternehmen (insgesamt das „Deloitte Netzwerk“) erbringen mittels dieser Veröffentlichung professionelle Beratungs- oder Dienstleistungen. Keines der Mitgliedsunternehmen des Deloitte Netzwerks ist verantwortlich für Verluste jedweder Art, die irgendjemand im Vertrauen auf diese Veröffentlichung erlitten hat.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL“), eine „private company limited by guarantee“ (Gesellschaft mit beschränkter Haftung nach britischem Recht), ihr Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen. DTTL und jedes ihrer Mitgliedsunternehmen sind rechtlich selbstständig und unabhängig. DTTL (auch „Deloitte Global“ genannt) erbringt selbst keine Leistungen gegenüber Mandanten. Eine detailliertere Beschreibung von DTTL und ihren Mitgliedsunternehmen finden Sie auf www.deloitte.com/de/UeberUns.

Deloitte erbringt Dienstleistungen in den Bereichen Wirtschaftsprüfung, Risk Advisory, Steuerberatung, Financial Advisory und Consulting für Unternehmen und Institutionen aus allen Wirtschaftszweigen; Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Mit einem weltweiten Netzwerk von Mitgliedsgesellschaften in mehr als 150 Ländern verbindet Deloitte herausragende Kompetenz mit erstklassigen Leistungen und unterstützt Kunden bei der Lösung ihrer komplexen unternehmerischen Herausforderungen. Making an impact that matters – für die rund 457.000 Mitarbeiter von Deloitte ist dies gemeinsames Leitbild und individueller Anspruch zugleich.