Abteilung Digitale Arbeitswelten und Arbeitsweltberichterstattung
Abteilung Recht

21. Juni 2021

Erste Einschätzung
der arbeitspolitisch relevanten Aspekte zum

Entwurf der EU-Kommission (EU KOM) für eine europäische KI-Verordnung
(ARTIFICIAL INTELLIGENCE ACT) vom 21. April 2021

1) Der DGB begrüßt grundsätzlich,
dass die EU KOM KI-Systeme im Kontext von Arbeit und Beschäftigung grundsätzlich als Hochrisiko einstuft und damit an besondere Zulassungsbedingungen bindet. Dazu gehören KI-Systeme, die „bei der Beschäftigung, dem Management von Arbeitnehmern und dem Zugang zur Selbstständigkeit eingesetzt werden, insbesondere für die Einstellung und Auswahl von Personen, für Entscheidungen über Beförderung und Kündigung sowie für die Aufgabenzuweisung, Überwachung oder Bewertung von Personen" (Erwägungsgrund 36). Unklar ist dabei jedoch, ob die über digitale Plattformen organisierte Arbeit in den Geltungsbereich dieser Verordnung fällt. Dies ist zu bewährleisten.

   Der DGB begrüßt ebenso grundsätzlich,
dass KI-Systeme, die „in der allgemeinen oder beruflichen Bildung eingesetzt werden, insbesondere zur Bestimmung des Zugangs oder der Zuweisung von Personen zu Bildungs- und Berufsbildungseinrichtungen oder zur Bewertung von Personen anhand von Tests als Teil oder Voraussetzung für ihre Ausbildung (vgl. Erwägungsgrund 35), als Hochrisiko eingestuft werden.

2) Der DGB kritisiert jedoch,
die von der EU KOM geplante, massive Eingrenzung der Hoch-Risiko-Einstufung durch ‚Annex III' auf (a) KI-Systeme bei Einstellung, Auswahl (insbesondere Ausschreibung freier Stellen), dem Screening oder Filtern von Bewerbungen, der Bewertung von Bewerbungen im Rahmen von Vorstellungsgesprächen oder Tests als auch auf (b) Entscheidungen über Beförderung oder Beendigung von Arbeitsverhältnissen; bei der Aufgabenzuweisung und bei der Überwachung und Bewertung von Leistungen und des Verhaltens.

Der DGB fordert stattdessen,
dass KI-Systeme grundsätzlich als Hochrisiko eingestuft werden, wenn personenbezogene Daten im Beschäftigungsverhältnis tangiert sind. Dies betrifft sowohl die Sphäre der Personalverwaltung (einschließlich der Anbahnung von Arbeitsverhältnissen) inklusive der Einbeziehung der Sozialversicherungssysteme als auch und insbesondere die Interaktion von Beschäftigten mit KI-Systemen im Arbeitsprozess (z. B. Embodied Intelligence). Nur so können Abgrenzungsfragen vermieden werden, die sich vor allem auf neue Formen der Mensch-Maschine-Interaktion oder Mensch-Roboter-Kollaboration beziehen oder algorithmische Steuerungsformen implizieren. Ob dies ist durch die sektoral passende Maschinenverordnung aufgefangen werden kann, ist zu klären.

Der DGB fordert zudem,
dass Analyse-Verfahren im HR-Bereich, die Beschäftigte zum Objekt machen, indem Daten erhoben werden, die willentlich nicht steuerbar sind, rechtlich auszuschließen sind (Kategorie „Unannehmbares Risiko").

Der DGB fordert weiter,
eine rechtliche Regelung, nach der die Nutzung personenbeziehbarer Daten im Beschäftigungskontext bei KI-Nutzung nicht allein eine individuelle Einwilligung voraussetzt, sondern zusätzlich auch eine kollektivrechtliche Vereinbarung, die eine transparente Zielsetzung, Einsichts- und Nutzungsregelungen sowie deren Grenzen beinhaltet. Gibt es keinen Betriebsrat oder keine Tarifbindung, so könnte die Zustimmung einer Behörde konkret eingeholt werden oder die "kollektivrechtliche Genehmigung" anhand von Regelbeispielen, die die Aufsichtsbehörde formuliert hat, erteilt werden.

3) Der DGB kritisiert,
dass der Vorschlag der EU KOM keinerlei Prozessvorgaben zu Mitwirkungs- und Mitbestimmungsmöglichkeiten für die betriebliche Anwendung von KI-Systemen beinhaltet. Dies betrifft die Beteiligung der Sozialpartner, die Mitbestimmung sowie die Partizipation von betroffenen Beschäftigten. So hatte die EU KOM auch im Weißbuch zum Regulierungsvorschlag 2020 festgestellt, dass „die Einbeziehung der Sozialpartner […] entscheidend zu einem menschenzentrierten KI-Konzept für den Arbeitsplatz" beiträgt. In dem nunmehr vorgelegten Entwurf findet die Beteiligung der Sozialpartner keine Erwähnung mehr.

Der DGB fordert deshalb,
prozessuale Nutzungsvorgaben im betrieblichen Einsatz zur Ermöglichung einer präventiven, diskriminierungsfreien, gendersensiblen und ganzheitlichen Arbeitsgestaltung, die insbesondere eine betriebliche Folgenabschätzung (Risk Management System), die vorgesehenen Testing-Verfahren (Art.7 (5)), das Quality Management system (Art.17) für ausreichende Transparenz und Nachvollziehbarkeit sowie eine kontinuierliche Evaluation der lernenden Systeme im Betrieb und Interventionsmöglichkeiten einschließen. Die Berücksichtigung von Kollektivvereinbarungen kann und sollte analog zur DSGVO (Art. 88) integriert werden. Die Auswirkungen auf die betrieblichen Arbeitsprozesse (Beschäftigungsaussichten, Profilveränderungen, Arbeitsschutz etc.) sind ausdrücklich bei dem für Hochrisiko-Anwendungen geforderte ‚Risikomanagement-System' zu berücksichtigen. Die Mitgestaltungsmöglichkeiten der Beschäftigten und deren Interessenvertretungen sind dabei dringend zu stärken und verbindlich prozesshaft auszurichten, um Zielkonflikte sozialverträglich zu lösen und unintendierte Nebeneffekte im Arbeitsleben zu vermeiden, die den europäischen Werten widersprechen. Es sollte klar geregelt sein, dass der betriebliche Einsatz nur unter zwingender Beteiligung der Interessenvertretungen der Beschäftigungen erfolgen kann, etwa durch Abschluss von Kollektivvereinbarungen. Dies muss für die Einführung ebenso wie für die betriebliche Ausgestaltung gelten. Der Zugriff von Arbeitnehmervertretungen auf die relevanten Informationen muss auch entlang der „Lieferkette" von AI, also bis zum „provider" sichergestellt werden.

Der DGB fordert,
dass die von den Beschäftigten erlernten, individuellen Fähigkeiten in der Interaktion mit KI-Systemenn für sie nutzbar sind, um die Portabilität des Know-hows zu ermöglichen.

4) Der DGB fordert
ein Verbandsklagerecht für Gewerkschaften im ersten Schritt für die Offenlegung der Funktionsweisen der Algorithmen bei betrieblich genutzten KI-Systemen sowie des Quellcodes hinter diesen Algorithmen. Ein solcher einklagbarer Anspruch auf Offenlegung für Gewerkschaften ist notwendig, um auch die durch KI-Systeme kollektiv erfassten Daten prüfen und damit etwaige Schäden von den Beschäftigten abwenden zu können. Darüber hinaus ist zu gewährleisten, dass arbeitsrechtliche Sanktionen für Beschäftigte, die sich theoretisch aus der Interaktion mit KI-Systemen ergeben können (insb. beim Umgang mit Entscheidungsvorschlägen), verbindlich auszuschließen sind.

5) Der DGB kritisiert,
dass nach dem Vorschlag der EU KOM durch Art. 43 mit Bezug auf Annex III für die Umsetzung der Auflagen für KI-Anbieter im Kontext der Arbeit eine Einrichtung von unabhängigen Stellen und entsprechender Audits für den Bereich der Arbeit explizit nicht vorgesehen ist.

Der DGB fordert,
insbesondere für den Bereich von Arbeit und Beschäftigung unabhängige KI-Agenturen zur Unterstützung der betrieblichen Akteure bei Beratung, Testung, Prüfung und Beschwerden auf nationaler Ebene einzurichten, die mit ausreichenden Ressourcen ausgestattet sein müssen.

6) Die Einrichtung einer europäischen KI-Behörde (European Artificial Intelligence Board Titel VI Chapter 1 Art. 56 ff) erscheint angesichts der Fülle an Koordinierungs- und Steuerungsaufgaben, die unmittelbar in Folge der Schaffung eines einheitlichen Regelungsrahmens für den Einsatz von KI entstehen werden, folgerichtig.

7) Die Sanktionsregelung des Art. 71 der Verordnung ähnelt in ihrer Systematik der DSGVO: die maximale Bußgeldhöhe orientiert sich an dem weltweiten Jahresumsatz eines Unternehmens. Dies ist zu begrüßen, denn es verspricht – bei effizienten Ahndung – hinreichend abschreckende Wirkung. Für effektive Strafen, die bei Verstößen vorgesehen werden sollten (Erwägungsgrund 84) um effektiven Schutz von Beschäftigtenrechten zu sichern, sollten die Strafen eine bestimmte Mindesthöhe haben.

Weitere zu klärende Fragestellungen:

- Rechtssichere Begrifflichkeit bei „Klassifizierung"

  Die Verordnung räumt der EU-Kommission in Art. 7 die ergänzende Kompetenz, anhand von unbestimmt definierten Kriterien die Liste der high-risk Systeme in Annex III zu ergänzen. Die Kriterien sowie die Einordnung, die hier zu Anwendung kommen sollen, erfordern ein transparentes und demokratisch kontrolliertes Verfahren.

  Die Regelung der „verbotenen" KI-Anwendungen in Art. 5 enthält viele unbestimmte Rechtsbegriffe, was viel Interpretationsspielraum lässt. Es stellt sich zum Beispiel die Frage, ob sich rechtssicher KI-Systeme bestimmen lassen, die die Schwächen einer Person mit körperlicher Behinderung ausnutzen, um ihr Verhalten mit der Folge eines psychischen Schadens zu beeinflussen. Es muss gewährleistet werden, dass die Auswertung gewerkschaftlicher Betätigung im öffentlichen Raum mithilfe von KI als Union Busting Strategie zu unterbinden ist.

  Weitere Relevanz für die Arbeitswelt und damit der Einstufung als high risk haben folgende Bereiche: Sozialrecht (Erwägungsgrund 37), „law enforcement authorities" (Erw. 38), border control management (Erw. 39) und administration of justice and democratic processes (Erw. 40). Es ist zu begrüßen, dass KI-Systeme, die für die Verwaltung oder für demokratische Prozesse vorgesehen sind, als Hochrisiko eingeschätzt werden. Im Hinblick auf Betriebsratswahlen sollten KI-Systeme nur unter engen Voraussetzungen zulässig sein.

  Zu begrüßen ist, dass die Regeln auch für Anwendungen gelten sollen, die außerhalb der EU errichtet wurden. Das trifft auf viele in der Arbeitswelt eingesetzte Systeme bereits jetzt zu. Problematisch ist die Ausnahme des Art. 2 Abs. 4 – vollständige Ausnahme von Behörden aus Drittstatten und internationaler Einrichtungen, die auf dem Gebiet der Rechtsdurchsetzung tätig sind. Gerade bei Strafverfolgung und polizeilichen Maßnahmen kann ein unbegrenzter und ungeregelter Einsatz von KI u. U. zu massiven Rechtverletzungen führen.

  Unklar ist, ob und welcher Mechanismus greifen soll, wenn eine high-risk Anwendung im Zuge des „Lernens" (also der datenbasierten Fortentwicklung seiner Eigenschaften) die Kriterien eine „verbotenen" Systems entwickelt, also z.B. anhand der gesammelten Daten das Verhalten einer Person unterschwellig beeinflussen kann. Dazu enthalten weder die Regelungen des Titel II (verbotene Anwendungen) noch des Titel III (high-risk Anwendungen) Lösungsmechanismen.

- Einführung biometrischer Echtzeitüberwachung „durch die Hintertür" – auch im Arbeitsleben

  Problematisch ist die mit der generellen Ausnahme des Art. 2 Abs. 4 korrespondierende Ausnahme nach Art. 5 Abs. 1 lit. d der Verordnung, welche die Verwendung von biometrischen Fernidentifizierungssystemen in "Echtzeit" in öffentlich zugänglichen Räumen zum Zweck der Strafverfolgung zulässt, etwa für die Abwehr einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder einer terroristischen Gefahr. Damit wird der Ausbau der Überwachungsmöglichkeiten mittels Erhebung biometrischer Echtzeitdaten, etwa mit dem Argument einer permanenten Gefahr für körperliche Unversehrtheit etwa im Zuge der Pandemie, legitimiert. Beschäftigte. die im öffentlichen Raum ihrer Arbeit nachgehen – beispielsweise bei der Polizei, den Rettungsdiensten, der Stadtreinigung oder im Personennaheverkehr – würden auch im Arbeitsverhältnis von Überwachungsmöglichkeiten erfasst werden, die weiter gehen, als die auf Grundlage des Datenschutzrechts zulässige Überwachung im Arbeitsverhältnis. Die Kriterien, die im Anschluss (unter Art. 5 Abs. 2) die Zulässigkeit der biometrischen Überwachung in Echtzeit konditionieren, sind sehr vage gehalten und nicht wirklich justitiabel. Auf dieser Grundlage droht eine unionsweite Legitimation biometrischen Überwachungsmöglichketen im öffentlichen Raum.

- Datenzugang

  Aus Sicht des DGB besteht Diskussionsbedarf in Bezug auf den Zugang zu den Datensets (Erwägung 45). Sozialpartner und Betriebsräte brauchen als relevante Akteure Zugang zu den Daten, insbesondere zu den Dokumentationen bei high-risk-Anwendungen (Erw. 48).

- Verhältnis Verordnung zu nationalen Regelungen

  Die Verordnung beschränkt die Kompetenzen der nationalen Regelungsgeber bei der Entscheidung über die Zulassungsbedingungen von KI-Anwendungen. Im Mittelpunkt der Verordnung stehen umfangreiche technische Vorgaben sowie Regelungen des Zulassungs- und Zertifizierungsverfahrens für high-risk KI-Anwendungen, zu den auch solche gehören, die im Zusammenhang mit Beschäftigungsverhältnissen eingesetzt werden. Nach dem Erwägungsgrund 67 sollen die Mitgliedstaaten bei den nach der Verordnung zulässigen high-risk-KI-Systeme nicht mehr berechtigt sein, deren Nutzung oder deren Einsatz einzuschränken. Sobald also zum Beispiel eine Personalauswahl-Anwendung ein Zulassungsverfahren nach Art. 43 der Verordnung durchgelaufen hat sowie eine CE-Zertifizierung nach Art. 48, 49 der Verordnung besitzt, ist im nationalen Kontext deren Einsatzeinschränkung dem Grundsatz nach nicht möglich. Nicht eindeutig ist in diesem Zusammenhang inwieweit die Verordnung die Entscheidungsprärogative der mitgliedstaatlichen Akteure über den Einsatz und Nutzung bestimmter KI-Anwendungen in der betrieblichen Praxis einschränkt. Wörtlich heißt es in EG 67: "*High-risk AI systems should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to the placing on the market or putting into service of high-risk AI systems that comply with the requirements laid down in this Regulation and bear the CE marking"*. Unter der Formulierung "putting into service" ist gemäß Art. 3 Nr. 11 „die Lieferung eines

KI-Systems zur erstmaligen Verwendung direkt an den Nutzer für den vorgesehenen Zweck" zu verstehen, also der Einsatz beim Anwender. Vor diesem Hintergrund ist eine Klarstellung erforderlich: Die Entscheidung über den Einsatz von KI-Anwendungen, die den Anforderungen der Verordnung entsprechen und insofern den Markzugang erlangen, muss den Akteuren in den Mitgliedstaaten, darunter auch den betrieblichen Akteuren überlassen blieben. Das erscheint auch – soweit die Speicherung, Verarbeitung und Weitergabe von Beschäftigtendaten tangiert ist – vor dem Hintergrund der Bestimmungen der DSGVO und der Möglichkeiten der nationalen Gesetzgeber, gem. Art. 88 DSGVO den Beschäftigtendatenschutz regulativ auszugestalten, zwingend. Da hinter die Standards der DSGVO nicht zurückgegangen werden darf, muss desgleichen auch für eine KI-Richtlinie gelten. So darf nicht – versteckt oder offen – durch die KI-Richtlinie der "DSGVO-Garantie" für die nationalen Regelungen zum Beschäftigtendatenschutz in Bezug auf die KI-Nutzung der Boden entzogen werden. Diese Klarstellung sollte ausdrücklich in die Verordnung aufgenommen werden.

- Anwendungsbereich

  Nach Art. 2 Abs. 1 lit. c soll die Verordnung für KI-Systeme gelten, die auf dem Markt der EU zur Anwendung kommen (lit.a), durch die Anwender innerhalb der EU genutzt werden (lit.b) oder mit einem output auf innerhalb der EU verbunden sind. Nicht ausdrücklich erfasst ist die oft in der Arbeitswelt anzutreffende Konstellation, dass in der Arbeitsbeziehung zwischen einem in der EU ansässigen Beschäftigten und seinem Arbeitgeber KI-Systeme zu Einsatz kommen, die außerhalb der EU eingerichtet wurden. Zwar stellt der Erwägungsgrund 10 der Verordnung klar, dass auch in diesem Fall die Regeln der Verordnung gelten sollen, diese Klarstellung bleibt aber rechtlich unverbindlich. Der Anwendungsbereich der Verordnung sollte daher rechtsverbindlich auch solche Fallkonstellationen erweitert werden, bei denen Rechte und Interessen von EU-Bürgern betroffen sind, auch wenn der Output (Arbeitsergebnis) in einem Drittstaat (etwa bei Unternehmenssitzen / Plattformanmeldung außerhalb der EU) entsteht.

- Die Bewertung der sehr umfangreichen Regelungen der technischen Anforderungen an die KI-Systeme, der Überprüfungs- und Zulassungsmechanismen (Titel IV, Chapter 3 – 5) ist ohne technische Expertise nicht möglich. Daher wird dieser sehr umfangreiche Teil noch zu ergänzen sein.

Hintergrund

Risiko basierter Ansatz des Kommissionsvorschlags

Der durch die EU-Kommission vorgestellte Entwurf für einen Rechtsrahmen für KI beruht auf einem vierstufigen risikobasierten Ansatz:

- **Unannehmbares Risiko**: KI Anwendungen, die gegen die Werte der EU verstoßen, sollen verboten werden. Dies betrifft die Bewertung des sozialen Verhaltens durch Behörden (Social Scoring), die Ausnutzung der Schutzbedürftigkeit von Kindern, Techniken zur unterschwelligen Beeinflussung und, mit engen Ausnahmen, biometrische Echtzeit-Fernidentifizierungssysteme, die zu Strafverfolgungszwecken im öffentlichen Raum eingesetzt werden sollen.

- **Hohes Risiko**: KI-Systeme die sich nachteilig auf die Sicherheit der Menschen auswirken können. Zu solchen Systemen gehören auch Sicherheitskomponenten von Produkten, die unter sektorale Rechtsvorschriften der Union fallen. Es wird stets davon ausgegangen, dass von ihnen ein hohes Risiko ausgeht, wenn sie gemäß diesen sektoralen Rechtsvorschriften einer Konformitätsbewertung durch Dritte unterzogen werden müssen.

  Eine Hochrisiko-Bewertung liegt in den folgenden Bereichen vor:

  a) kritische Infrastrukturen (z. B. im Verkehr), in denen das Leben und die Gesundheit der Bürger gefährdet werden könnten;

  b) Schul- oder **Berufsausbildung**, wenn der Zugang einer Person zur Bildung und zum Berufsleben beeinträchtigt werden könnte (z. B. Bewertung von Prüfungen);

  c) Sicherheitskomponenten von Produkten (z. B. eine KI-Anwendung für die roboterassistierte Chirurgie);

  d) Beschäftigung, Personalmanagement und Zugang zu selbstständiger Tätigkeit (z. B. Software zur Auswertung von Lebensläufen für Einstellungsverfahren);

  e) wichtige private und öffentliche Dienstleistungen (z. B. Bewertung der Kreditwürdigkeit, wodurch Bürgern die Möglichkeit verwehrt wird, ein Darlehen zu erhalten);

  f) Strafverfolgung, die in die Grundrechte der Menschen eingreifen könnte (z. B. Bewertung der Verlässlichkeit von Beweismitteln);

  g) Migration, Asyl und Grenzkontrolle (z. B. Überprüfung der Echtheit von Reisedokumenten);

  h) Rechtspflege und demokratische Prozesse (z. B. Anwendung der Rechtsvorschriften auf konkrete Sachverhalte)

- **Geringes Risiko**: bestimmte KI-Systeme müssen Transparenzpflichten erfüllen, wenn Manipulationsgefahr besteht (etwa Einsatz von Chatbots). Hier muss gekennzeichnet sein, das die Kommunikation mit einer Maschine erfolgt.

- **Minimales Risiko**: dies betrifft KI-Systeme, die nicht den vorher genannten Klassifizierungen unterstellt sind. Hier soll die Möglichkeit geschaffen werden, sich einer freiwilligen „Zertifzierung" als vertrauensvolle KI zu unterziehen und freiwillige Verhaltenskodizes einzuhalten.

KI-Systeme sollen laut EU-KOM **im Kontext Arbeit** als **Hochrisiko** eingestuft werden, wenn:

- KI-Systeme **in der allgemeinen oder beruflichen Bildung** eingesetzt werden, insbesondere zur **Bestimmung des Zugangs oder der Zuweisung von Personen zu Bildungs- und Berufsbildungseinrichtungen oder zur Bewertung von Personen** anhand von Tests als Teil oder Voraussetzung für ihre Ausbildung (vgl. S. 26 Punkt 35)

- KI-Systeme **bei der Beschäftigung, dem Management von Arbeitnehmern und dem Zugang zur Selbstständigkeit** eingesetzt werden, insbesondere für die **Einstellung und Auswahl von Personen, für Entscheidungen über Beförderung und Kündigung sowie für die Aufgabenzuweisung, Überwachung oder Bewertung von Personen** (vgl. S. 26 Punkt 36)

Der **Annex III** (S. 4) konkretisiert dies weiter:

a) KI Systeme **bei Einstellung, Auswahl** (insbesondere Ausschreibung freier Stellen), dem Screening oder Filtern von Bewerbungen, der **Bewertung von Bewerbungen** im Rahmen von Vorstellungsgesprächen oder Tests

b) KI bei **Entscheidungen über Beförderung oder Beendigung von Arbeitsverhältnissen**; bei der **Aufgabenzuweisung** und bei der **Überwachung und Bewertung von Leistungen und des Verhaltens**

Für KI-Systeme / Anbieter[1] in der Hochrisiko-Einstufung sind dabei folgende Anforderungen gestellt

- angemessene Risikobewertungs- und Risikominderungssysteme
- hohe Qualität der Datensätze, die in das System eingespeist werden, um Risiken und diskriminierende Ergebnisse so gering wie möglich zu halten
- Protokollierung der Vorgänge, um die Rückverfolgbarkeit von Ergebnissen zu ermöglichen
- ausführliche Dokumentation mit allen erforderlichen Informationen über das System und seinen Zweck, damit die Behörden seine Konformität beurteilen können
- klare und angemessene Informationen für die Nutzer
- angemessene menschliche Aufsicht zur Minimierung der Risiken
- hohes Maß an Robustheit, Sicherheit und Genauigkeit

Provider von KI-Anwendungen müssen bei Hochrisiko-Einstufungen ein Risikomanagement-System einrichten, dokumentieren und aufrechterhalten, das über den gesamten Lebenszyklus des KI-Systems abläuft und regelmäßig aktualisiert werden muss.
Die Aufgaben sind unter Artikel 9 (S.46) beschrieben und enthalten z. B.:

- Identifizierung und Analyse der bekannten und vorhersehbaren Risiken, die mit jedem KI-System mit hohem Risiko verbunden sind
- Abschätzung und Bewertung der Risiken, die bei bestimmungsgemäßer Verwendung des KI-Systems mit hohem Risiko und bei vernünftigerweise vorhersehbarer Fehlanwendung entstehen können

Provider von KI-Anwendungen müssen nach Artikel 17 (vgl. S. 53) bei Hochrisiko-Einstufungen ein Qualitätsmanagement-System einführen mit der die Einhaltung der Vorschriften dokumentiert wird. Die zu dokumentierenden Aspekte sind ebenfalls unter Artikel 17 genannt.

Die Provider von Hochrisiko-KI müssen laut Artikel 43 eine Konformitätsbewertung durchführen, zumeist ein internes Kontrollverfahren. Nur wenn bereits in sektoralen Rechtsvorschriften eine Konformitätsbewertung durch Dritte unterzogen wird oder laut Artikel 43 (Verweis Annex VII) die Biometrische Identifikation und Kategorisierung von natürlichen Personen tangiert wird, ist die Einrichtung einer unabhängigen Stelle dafür nötig. Unabhängige Audits über sog. ‚*notified bodies*' sind somit laut EU-KOM nicht für den Bereich Arbeit und Beschäftigung vorgesehen.

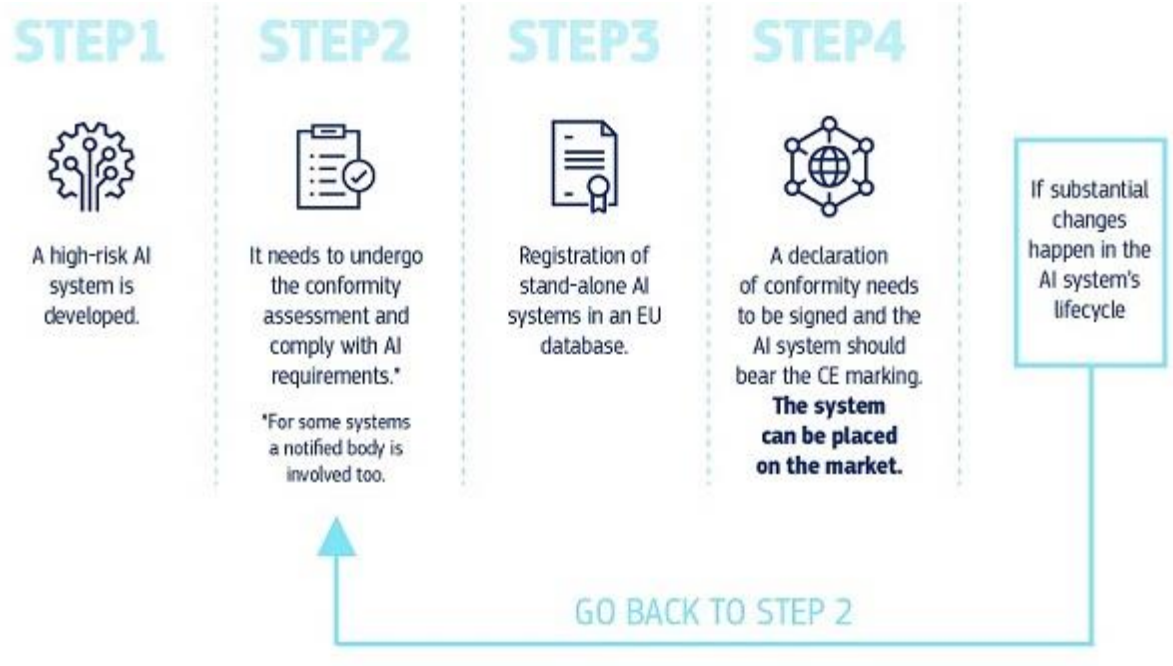
Die KI-Provider müssen die eigenständigen KI-Systeme in einer EU-Datenbank registrieren. Diese Registrierung wird es den zuständigen Behörden, Nutzern und anderen interessierten Personen grundsätzlich ermöglichen, zu überprüfen, ob das KI-System mit hohem Risiko die im Vorschlag festgelegten Anforderungen erfüllt. Um diese Datenbank zu speisen, werden die KI-Anbieter verpflichtet sein, aussagekräftige Informationen über ihre Systeme und die an diesen Systemen durchgeführte Konformitätsbewertung bereitzustellen. Über die CE-Zertifizierung sollen die KI-Anwender zudem sichtbar machen, dass sie die genannten Prozesse durchführen.

[1] Anbieter (Provider): eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System entwickelt oder entwickeln lässt, um es unter ihrem eigenen Namen oder ihrer eigenen Marke entgeltlich oder unentgeltlich in Verkehr zu bringen oder in Betrieb zu nehmen

Die Mitgliedsstaaten sollen bei der Anwendung und Durchsetzung der Verordnung eine oder mehrere nationale Behörden benennen. Um die organisatorische Effizienz auf Seiten der Mitgliedstaaten zu erhöhen und eine offizielle Kontaktstelle gegenüber der Öffentlichkeit und anderen Ansprechpartnern auf Ebene der Mitgliedstaaten und der Union zu schaffen, sollte in jedem Mitgliedstaat eine nationale Behörde als nationale Aufsichtsbehörde benannt werden. Die nationalen zuständigen Behörden und benannten Stellen, die an der Anwendung dieser Verordnung beteiligt sind, wahren die Vertraulichkeit von Informationen und Daten, die sie bei der Durchführung ihrer Aufgaben und Tätigkeiten erhalten haben, in einer Weise, dass insbesondere Folgendes geschützt wird: […] die wirksame Durchführung dieser Verordnung, insbesondere für die Zwecke von Inspektionen, Untersuchungen oder Audits (vgl. Art. 70) Nach Art. 23 stellen „die Anbieter von AI-Systemen mit hohem Risiko [...] der zuständigen nationalen Behörde auf deren Verlangen alle Informationen und Unterlagen in einer von dem betreffenden Mitgliedstaat festgelegten Amtssprache der Union zur Verfügung, die für den Nachweis der Konformität des AI-Systems mit hohem Risiko mit den Anforderungen [...] erforderlich sind." Voraussetzung ist allerdings die ausreichende kompetente Personalausstattung der nationalen Behörde(n) (Art. 30).

Zudem schlägt die Kommission die Einrichtung eines „European Artificial Intelligence Board" vor. Das Gremium soll die Durchführung der Verordnung erleichtern und Beratungsaufgaben übernehmen: Abgabe von Stellungnahmen, Empfehlungen, Ratschlägen oder Leitlinien zu Fragen im Zusammenhang mit der Durchführung dieser Verordnung, auch zu technischen Spezifikationen oder bestehenden Normen in Bezug auf die in dieser Verordnung festgelegten Anforderungen, und für die Beratung und Unterstützung der Kommission in spezifischen Fragen im Zusammenhang mit künstlicher Intelligenz (vgl. S. 35). Der Ausschuss setzt sich aus den nationalen Aufsichtsbehörden, die durch den Leiter oder einen gleichwertigen hochrangigen Beamten der jeweiligen Behörde vertreten werden, und dem Europäischen Datenschutzbeauftragten zusammen. Andere nationale Behörden können zu den Sitzungen eingeladen werden, wenn die erörterten Fragen für sie von Bedeutung sind (vgl. S.72).

Verfahrensvorschlag bei der Anwendung von KI mit hohem Risiko:



Kontakt:

Micha Klapp
Leiterin der Abteilung Recht
micha.klapp@dgb.de

Oliver Suchy
Leiter der Abteilung Digitale Arbeitswelten und Arbeitsweltberichterstattung
oliver.suchy@dgb.de