AK EUROPA

Positionspapier
Oktober 2021
Digitales

EU-Verordnung zur Künstlichen Intelligenz

COM(2021) 206

Zusammenfassung

2020 legte die EU Kommission das Weißbuch zur Künstlichen Intelligenz (KI) vor (siehe Positionspapier zum Weißbuch KI der Arbeitskammer). In Folge wurde nun ein Verordnungsentwurf zu KI von der Kommission erarbeitet.

Was ist gut am Entwurf?

Zu begrüßen ist, dass dieses zukunftsweisende Thema aufgegriffen wird, um einen Rahmen zu Förderung, Entwicklung und Einsatz, sowie zur Regulierung von KI zu schaffen. Es wurde dabei ein Ansatz gewählt, der unabhängig von der Technologie die Auswirkungen betrachtet und versucht eine Risikobewertung vorzunehmen. Daraus soll sich wiederum der Grad der Regulierungserfordernisse ableiten. Im Annex werden deshalb Beispiele von Anwendungen je Risikokategorie aufgelistet. Spätestens hierin ergeben sich jedoch eine Reihe von Fragen, denn die Risikoeinstufung ist entscheidend für die Gültigkeit von Regulierungsbestimmungen.

Welche Kritik ist angebracht, was fehlt?

Der Entwurf hat einen technikzentrierten Fokus mit Blick auf die Erfordernisse des Binnenmarkts. Der ursprünglich propagierte „menschenzentrierte Ansatz" findet sich kaum wieder. Wichtige Schutzmechanismen für Arbeitnehmer:innen und Konsument:innen fehlen, Möglichkeiten zur Mitbestimmung ebenso. Viele (richtige) Ansatzpunkte werden durch Ausnahmen und Einschränkungen verwässert, vieles bleibt unklar (zB. welche Kriterien müssen Systeme erfüllen, um überhaupt als KI zu gelten). Auch das institutionelle Setting der mit der Regulierung beauftragten Behörde(n) ist offen und entscheidend für den Umgang mit den Entwicklungen KI und ihren Risiken.

Was braucht es daher?

- Strenge Regulierung von KI-Anwendungen, die Arbeitnehmer:innenrechte, Arbeitsbedingungen und die Gesundheit am Arbeitsplatz berühren. Diese sollten prinzipiell als hochriskant eingestuft werden. Bestimmte – für Arbeitnehmer:innen besonders riskante – Anwendungen sollten nicht erlaubt sein.
- Das Prinzip der menschlichen Kontrolle.
- Weitgehende Transparenz, damit KI-Anwendungen verstanden und ihre Funktionsweisen erlernt werden können.
- Stärkung von Arbeitnehmer:innenbeteiligung in der Ausgestaltung, Entwicklung, Anwendung und Kontrolle von KI im Sinne eines menschenzentrierten „Bottom-Up-Ansatzes".
- Förderung betrieblicher und überbetrieblicher Aushandlungsprozesse durch eine Stärkung der Mitbestimmungsrechte.
- Konformitätsbewertung von KI-Systemen von autorisierten Stellen für Anwendungen im Bereich Arbeitnehmer:innen-Management, sowie Mechanismen, die Ex-Ante-Compliance und Ex-Post-Enforcement kombinieren.
- Begleitende Aus- und Weiterbildungen sowohl für betriebliche Interessenvertreter:innen als auch Arbeitnehmer:innen.
- Vorrang des Vorsichtsprinzips aufgrund unbekannter Risiken. Arbeitsunfällen und arbeitsbedingten Erkrankungen muss vorgebeugt werden und Arbeitnehmer:innen mit speziellen Bedürfnissen müssen mitbedacht werden. Die Aufsichtsbehörde (Arbeitsinspektion) braucht daher ausreichend Ressourcen, um die neuen Aufgaben abzudecken.
- Grund- und Persönlichkeitsrechte, Datenschutz, Arbeitnehmer:innenschutz und Konsument:innenrechte müssen Priorität haben und dürfen nicht durch Ausnahmen und Einschränkungen ausgehöhlt werden.

Die Position der AK

1. KI und Arbeitswelt

Allgemein: Vollständiges Fehlen des im Weißbuch angekündigten „menschenzentrierten Konzepts“

Mit ihrem **Vorschlag für einen Rechtsrahmen zur Künstlichen Intelligenz** strebt die Kommission an, dass die auf dem Unionsmarkt in Verkehr gebrachten und verwendeten KI-Systeme sicher sind und die **bestehenden Grundrechte und die Werte** der Union gewahrt werden. Zur Förderung von Investitionen in KI und Innovationen soll **Rechtssicherheit** gewährleistet sein. Governance und die wirksame Rechtsdurchsetzung zur Wahrung der Grundrechte sowie Sicherheitsanforderungen an KI-Systeme sollen gestärkt und die Entwicklung eines Binnenmarkts für rechtskonforme, sichere **und vertrauenswürdige KI-Anwendungen** erleichtert werden.

Noch in ihrer **Mitteilung vom 25.04.2018** bekannte sich die Kommission dazu, dass KI zu **Veränderungen in unserer Arbeitswelt** führt und die EU diesen Wandel steuern und begleiten muss; dass sie einen “**menschenzentrierten**”, **integrativen Ansatz für Künstliche Intelligenz** verfolgt und dass angesichts des Ausmaßes der mit KI verbundenen Herausforderungen ein breites Spektrum von Teilnehmer:innen (ua. Gewerkschaften) zu mobilisieren sind, um an **allen Aspekten** von KI zu arbeiten. **Die AK weist darauf hin, dass genau das nicht passiert ist und der Aspekt „Künstliche Intelligenz und Arbeitswelt“ mit seinen vielfältigen Herausforderungen in der vorgeschlagenen Verordnung nicht berücksichtigt wurde! Es fehlen spezielle Regelungen im Sinne von Schutzbestimmungen für betroffene Arbeitnehmer:innen bei der Anwendung von KI am Arbeitsplatz!**

Vor diesem Hintergrund **ist es bedenklich und enttäuschend, dass in der Verordnung primär ein rein technikzentrierter Ansatz gewählt wurde**. Arbeitnehmer:innen und deren Interessenvertretungen kommen dort als eigene Kategorien schlichtweg nicht vor. Im Weißbuch wurden wesentliche Gefahren, wie etwa Überwachung von Arbeitnehmer:innen, oder die Gefahr diskriminierender KI, dargestellt. Dies wurde von der AK in einem Positionspapier zum Weißbuch auch positiv gewürdigt. Umso wichtiger ist es, **beim Inverkehrbringen von KI am Arbeitsplatz einen Ansatz zu wählen, bei dem die Anwendungen (unter Einbeziehung von Arbeitnehmer:innen und ihrer Interessenvertretungen) gleichgewichtig das Ziel haben, Arbeit besser und humaner zu gestalten**. Es darf nicht alles zugelassen werden, was technisch möglich ist.

- Daher sollte der Einsatz von KI in der Arbeitswelt grundsätzlich als Hochrisikoanwendung gelten und bestimmte Anwendungen sollten gar nicht erlaubt sein.
- Im Falle des Inverkehrbringens solcher Hochrisikoanwendungen am Arbeitsplatz braucht es mehr als technische Rahmenbedingungen und Dokumentationspflichten. Arbeitnehmer:innen und ihren Interessenvertretungen müssen immer auch entsprechende Mitsprache- und Vetorechte zukommen.
- Für einen „menschenzentrierten“ KI-Ansatz, der auch die Auswirkungen der KI-Anwendungen auf die Arbeitswelt und Arbeitnehmer:innen im Fokus hat, wäre es unabdingbar, dass auch die Interessenvertretungen von Arbeitnehmer:innen und nicht nur die nationalen Behörden in den beratenden Gremien der Kommission vertreten sind (im Weißbuch wurde die Rolle der Sozialpartner noch hervorgehoben).

Lösungsansätze beim Einsatz von Künstlicher Intelligenz am Arbeitsplatz

KI-Systeme im Bereich Arbeitswelt und Beschäftigung wirken besonders einschneidend auf die Arbeitsbedingungen und können negative Auswirkungen auf Arbeitnehmer:innen haben. Diese Themen der Arbeitswelt und der Mitbestimmung werden in der Verordnung nicht einmal im Ansatz erwähnt. **Die wichtige Rolle der betrieblichen und überbetrieblichen**

Arbeitnehmer:inneninteressenvertretung bei der Einführung/Verwendung von KI am Arbeitsplatz, um das dort herrschende Machtungleichgewicht auszugleichen, gilt es explizit zu verankern!

Im Weißbuch wurde noch von einem "menschenzentrierten" KI-Ansatz gesprochen, die EK wies in Ansätzen auf Gefahren für Arbeitnehmer:innen hin. Nun fallen aufgezählte **KI-Anwendungen** etwa **bei Einstellungsverfahren** oder bei Entscheidungen über Beförderungen oder **Kündigungen**, für Aufgabenzuweisung sowie für die **Überwachung und Bewertung** von **Leistungen** und des **Verhaltens** von Personen in Beschäftigungsverhältnissen zwar unter Hochrisiko-KI-Systeme, nur sollen diese Anwendungen unter Einhaltung spezifischer Anforderungen und einer **ex-ante-Konformitätsbewertung auf der Grundlage interner Kontrollen zulässig sein. Damit wird aber zu wenig getan, um die Risiken zu begrenzen, die sich durch vielfältige Einsatzmöglichkeiten von KI-Anwendungen im Beschäftigungsverhältnis und aufgrund des dort herrschenden Machtungleichgewichts zwischen Arbeitgeber:innen und Arbeitnehmer:innen ergeben**. Augenscheinlich orientiert sich diese Verordnung primär an Technologieanbieter:innen, obwohl doch der Schutz der EU-Bürger:innen und der Arbeitnehmer:innen vorrangig sein müsste.

Zum Schutz von Arbeitnehmer:innen sind **Anwendungen, die auf Arbeitsrealitäten und -bedingungen negative Auswirkungen haben können, als „hochriskant" zu klassifizieren**. Insbesondere darf die vorzunehmende Konformitätsbewertung nicht ohne Einbeziehung der Betroffenen, das heißt der Arbeitnehmer:innen und ihrer Interessenvertretungen, erfolgen. **Bei der Einführung derartiger KI-Systeme am Arbeitsplatz sollte jede Bewertung von Risiken in Abstimmung mit den Interessenvertretungen der Arbeitnehmer:innen erfolgen. Werden die Risiken als zu hoch eingestuft, müssen diese von Anbieter:innen eliminiert werden, andernfalls dürfen die Systeme am Arbeitsplatz nicht eingesetzt werden**.

Bestimmte Anwendungen im Arbeitsverhältnis (automatisierte Entscheidungen im Einzelfall und Profiling) sollten aufgrund der besonders einschneidenden Auswirkungen auf die Arbeitsbedingungen überhaupt untersagt werden. Nach **Art 8 der EU-Grundrechtscharta** hat alle Anspruch auf Geheimhaltung seiner/ihrer Daten, soweit ein schutzwürdiges Interesse daran besteht. Beschränkungen des Anspruchs sind nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig. Aber selbst dann darf nur in der gelindesten Form ins Grundrecht eingegriffen werden. **In der Praxis des Arbeitsalltags erhält das Grundrecht oft nicht den Stellenwert, der ihm gebührt**. Die Entwicklung in der Personalverwaltung bzw. in der Betriebsorganisation geht in Richtung einer Datenökonomie, die nach immer mehr Daten für immer mehr Zwecke verlangt. **Die datenschutzrechtliche Lage für Arbeitnehmer:innen hat sich auch durch die DSGVO nicht maßgeblich verbessert**. Verstärkt wird dies zudem durch die EU-weite Förderung datengetriebener Wirtschaft. Angesprochen sind dabei Daten mit und ohne Personenbezug und solche, bei denen der Personenbezug entfernt wurde. Bezüglich letzterem räumen Expert:innen allerdings ein, dass Algorithmen durch maschinelles Lernen so gut wie jede Anonymisierung rückführen können und Arbeitnehmer:innen re-identifizierbar werden. Profiling, Scoring und Verhaltensprognosen sowie automatisierte Entscheidungsfindungen mit Hilfe von Algorithmen, maschinellem Lernen und KI können Arbeitnehmer:inneninteressen jedenfalls massiv gefährden. Arbeitnehmer:innenverhalten, persönliche Eigenschaften und vieles mehr dürfen nur aus besonderen, berechtigten Gründen und unter strikten Kautelen analysiert, klassifiziert oder prognostiziert werden. Unserer Auffassung nach **sind automatisierte Entscheidungen im Einzelfall und Profiling im Arbeitsverhältnis nicht erforderlich und dürfen daher nicht zulässig sein**. Dies hat auch für menschliche Entscheidungen „bloß" vorbereitende, „halbautomatisierte" Bewertungen zu gelten.

Arbeitnehmer:innen fürchten um die Wertschätzung für ihre menschliche Arbeit: Mit der „Übersetzung" aller Arbeitsbereiche in eine „Datenwelt" entsteht die Gefahr **im Arbeitsprozess zu einem technikzentrierten und damit inhumanen Menschenbild zu gelangen**. Die Arbeitsleistung der Arbeitnehmer:innen wird zunehmend in Zahlen ausgedrückt, gemessen, verglichen, analysiert und es werden daraus automatisiert Entscheidungen und Vorhersagen getroffen. Der Mensch am Arbeitsplatz wird zu einem messbaren Produktions- und Kostenfaktor herabgewürdigt. **Die Wahrung der Menschenwürde und der Persönlichkeitsrechte sind auch bei der Erbringung der Arbeitsleistung sicherzustellen, die Europäische Union muss dazu ein klares Bekenntnis abgeben!**

Herausforderungen beim Einsatz von KI am Arbeitsplatz

Die Verordnung entspricht in der Arbeitswelt leider keineswegs dem angekündigten „menschenzentrierten Ansatz". Nachstehend wird noch einmal auf die wichtigsten Herausforderungen

hingewiesen, **denen die Regeln für Anwendungen in der Arbeitswelt gerecht werden sollten**. Diese legen auch **Gründe dar, warum es explizit einen „menschenzentrierten" Ansatz braucht, der auf die bessere und humane Gestaltung der Arbeit und nicht nur auf die Gestaltung der Technik abzielt**:

- KI wird Arbeitsbedingungen einschneidend verändern. Die wirtschaftlichen Chancen, die sich durch den Einsatz von KI ergeben, sind zu nutzen, aber – aufgrund der Tatsache, dass damit auch technische Möglichkeiten zur **Überwachung am Arbeitsplatz** und zur Verwendung von Arbeitnehmer:innendaten zunehmen – müssen **die Rechte der Beschäftigten durch konkrete Regelungen geschützt werden!**

- IT/KI-Systeme (Laptop, Smartphone, vernetzte Maschinen, Programme zur Personalverwaltung und Betriebsorganisation) werden immer komplexer. **Die Menge der dabei generierten und verwendbaren Beschäftigtendaten nimmt exponentiell zu und die technischen Verknüpfungs- und Analyse-Möglichkeiten dieser Daten werden immer ausgereifter und aussagekräftiger** – bis hin zum Erstellen von Bewertungen und Verhaltensvorhersagen von Arbeitnehmer:innen (Profiling) und dem Einsatz automatisierter Entscheidungsfindungen.

- **Entscheidend für den Schutz von Arbeitnehmer:innen sind vor allem Mitbestimmungsrechte der betrieblichen und überbetrieblichen Interessenvertretungen bei der Einführung von KI am Arbeitsplatz**: Das können Informations-, Mitgestaltungs- und Zustimmungs- bzw. Vetorechte der einzelnen Beschäftigten, aber vor allem auch – angesichts der Verhandlungsunterlegenheit der einzelnen Beschäftigten gegenüber der/dem Arbeitgeber:in – von betrieblichen und überbetrieblichen Interessenvertretungen sein.

- Hervorgehoben sei auch, dass **eine allfällige Zustimmung der Arbeitnehmer:innen zur Verwendung ihrer personenbezogenen Daten in der Regel nicht freiwillig erfolgen kann, weil sich im Arbeitsverhältnis keine gleichberechtigten Vertragspartner:innen gegenüberstehen**. Die Praxis zeigt, dass Arbeitnehmer:innen im aufrechten Arbeitsverhältnis ihre Rechte so gut wie nie einfordern (können). Um dem entgegenzuwirken, braucht es **starke Mitbestimmungsrechte der Interessenvertretungen** bei der Einführung von KI am Arbeitsplatz und ein explizites Verbandsklagerecht der überbetrieblichen Interessenvertretung zur Stärkung der Rechtsdurchsetzung.
  Zudem erfolgt die **Beauskunftung von Datenverarbeitungen oft mangelhaft und in einer nicht leicht verständlichen Sprache, womit Transparenz, Information und Nachvollziehbarkeit bei den Arbeitnehmer:innen und ihren Interessenvertretungen in der Praxis in den seltensten Fällen ausreichend gegeben ist** (so erfolgt die Befragung der betroffenen Arbeitnehmer:innen und ihrer Interessenvertretungen bei der Datenschutz-Folgenabschätzung nach der DSGVO meist ungenügend oder unterbleibt ganz).

- Um die positiven Potenziale von KI auch für Arbeitnehmer:innen zu heben und sie dennoch vor Gefahren zu schützen, bedarf es eines **„Bottom-Up-Ansatzes", bei dem nicht nur die technischen Grundlagen und Anwendungen der Mitbestimmung unterzogen werden, sondern bei dem von Beginn an die Auswirkungen von KI auf arbeitende Menschen und deren Arbeitsbedingungen untersucht werden und über den endgültigen Einsatz erst auf Basis dieser Erfahrungen entschieden wird**. Zumindest ein klares Bekenntnis der Europäischen Kommission zu einem solchen Ansatz wäre wünschenswert, damit in der operativen Umsetzung auch die entsprechende Position der Arbeitnehmer:innenvertretung und damit die Arbeitnehmer:innenrechte berücksichtigt werden können.

2. KI und Konsument:innen

Die Absicherung eines hohen Verbraucher:innenschutzniveaus ist auch bei Algorithmen und KI wichtig. **Konsument:innen müssen vor einer Aushöhlung ihrer Grund- und Freiheitsrechte, Intransparenz, Diskriminierung, körperlichen sowie psychischen Risiken und sonstigen Schadensrisiken, die von derartiger Analysesoftware ausgehen**, bestmöglich geschützt werden. Dazu sind folgende Punkte erforderlich:

- **Regeln nicht nur für Hochrisiko-KI**: Auch bei „bloß" riskanten Anwendungen sind Transparenz, Diskriminierungsfreiheit, Beschwerderechte durch Vorschriften abzusichern.

- **Verankerung von Rechten für betroffene Bürger:innen und Verbraucher:innen**: ua. das Recht auf Information, Auskunft, Selbstbestimmung, Beschwerderechte.

- **Verbot von gesellschaftlich unerwünschten KI-Systemen** statt lückenhafter Verbote einiger Spielarten von Social Scoring, biometrischer Fernüberwachung und Verhaltensmanipulation.

- **Konkrete Benennung von Risiken**: Für hochriskante KI finden sich zwar Hinweise auf Gefahren für die Sicherheit, Gesundheit und Grundrechte. Doch ist weder ein Diskriminierungsverbot verankert noch genau normiert, in welchem risikofreien bzw. -behafteten Zustand KI auf den Markt gelangen darf.

- **Schließen von Schlupflöchern im korrespondierenden Art 22 DSGVO** bezüglich algorithmischer, automatischer Einzelentscheidungen.

- **KI-Zertifizierung ausnahmslos durch unabhängige Behörden** statt bloßer Selbstzertifizierung durch die Hersteller.

- **KI-Entscheidungen, -Dienste und –Produkte müssen erklär- und überprüfbar bleiben.**

- **Schutznormen für biometrische KI-Analysen bei Verbraucher:innengeschäften.**

- **keine Ausnahmen von der DSGVO für den Dateneinsatz in KI-„Reallaboren".**

- **Institutionelle Einbindung der Betroffenen.**

- **Überarbeitung der unzeitgemäßen Regeln für Produkthaftung und Produktsicherheit**, um sie „KI-fit" zu machen.

- **kollektive Rechtsschutzmöglichkeiten für Betroffene ua. durch Verbandsklagsbefugnisse.**

Allgemeine konsument:innenpolitische Defizite des Entwurfes

Verbraucheranliegen werden nicht mitgedacht: Konsument:innen werden durch Algorithmen oft kategorisiert und bewertet. Intransparenz, Grundrechtsverletzungen, Benachteiligung, Verhaltensmanipulation und Überwachung entstehen auch bei der Nutzung smarter Dienste und Güter. KI kann auch aus anonymisierten Datensätzen Personen identifizieren, klassifizieren, oder als Informationsfilter Meinungen beeinflussen. Gesetzliche Anforderungen sind deshalb nicht nur für Hochrisiko-KI, sondern für alle KI-Anwendungen angemessen.

„KI muss vertrauenswürdig sein!": Die vorgesehenen Rechtsinstrumente für Bedrohungsszenarien sind schwach, denn laut Kommission sollen keine „unverhältnismäßig hohen Bürden" entstehen. Man setzt primär auf die Regulierung von hochriskanter KI. Ob ein Schaden von einer hochriskanten oder bloß risikobehafteten KI herrührt ist für Verbraucher:innen jedoch irrelevant. Vorabkontrolle, Transparenz- und Beschwerderechte sind in jedem Fall notwendig.

Skepsis gegenüber „ethischer" Technik angebracht: Der Philosoph Richard David Precht (Künstliche Intelligenz und der Sinn des Lebens) spricht vom „Irrsinn, Maschinen Ethik einzuprogrammieren". Unmissverständliche Verbote seien nötig: „Besonders in ethisch sensiblen Bereichen" bestehe „die Gefahr, dass wir Maschinen sehr weitreichende Handlungsvollmachten übertragen, die sie auf keinen Fall bekommen dürfen".

Benötigt werden klare Ge- bzw. Verbote: Klare Grenzen und rote Linien werden in der VO oft nicht gesetzt. Was fehlt sind Verbote ohne vielfältige Ausnahmen, Risikobenennung (auch bei Diskriminierungsgefahren), Selbstbestimmungsrechte darüber, ob KI die eigene Person betreffende Entscheidungen treffen darf, Informationspflichten, behördliche Vorabprüfung der Folgen für Menschenwürde und Freiheitsrechte, Produktsicherheit und -haftung sowie außergerichtliche Beschwerdestellen und Verbandsklagsbefugnisse.

Der bloßer Verweis auf die in Art 22 DSGVO enthaltenen Rechte reicht dabei keinesfalls aus (siehe AK-Stellungnahme zur Evaluation der Datenschutz-Grundverordnung).

KI ähnelt einer Blackbox. Auch Expert:innen können oft nicht genau erklären, warum eine KI zu bestimmten Ergebnissen gelangt. Kann man KI-Ergebnisse aber nicht verantworten, weil man sie selbst nicht begreift und beherrscht, ist aus Sicht der AK eine Anwendung zu verbieten.

Transparenz: Transparenzverpflichtungen gelten nur für professionelle Anwender:innen von KI Systemen. Gegenüber Endnutzer:innen und Konsument:innen sind kaum welche festgeschrieben. Wer nicht weiß, wo und wie KI-Systemen eingesetzt werden, kann aber auch nicht abschätzen, ob und wie er/sie davon betroffen ist. Die DSGVO schafft hier auch keine Abhilfe, weil sie nur bei personenbezogenen Daten bzw. bei vollautomatisierten Einzelentscheidungen Informations- und Auskunftspflichten vorsieht.

Fehlender Rechtsschutz: Komplexe Algorithmen und maschinelle Selbstlernfähigkeit werden die

zuständigen Aufsichtsbehörden und Gerichte weit über ihre Grenzen fordern, was zu Lasten des Rechtschutzes geht.

Außergerichtliche Anlaufstellen: Zulassungen und Konformitätsentscheidungen eines Mitgliedsstaates sind in der gesamten EU wirksam. Wenn die Niederlassungsstaaten von Herstellern, Nutzer:innen und Verbraucher:innen auseinanderfallen, führt das zu Problemen. Es braucht niedrigschwellige Rechtsschutzmechanismen für Betroffene, um grenzüberschreitende Informationen einfordern oder Beschwerden tätigen zu können.

Mehr Prävention: Konsument:innen und Arbeitnehmer:innen erwarten sich einen vorbeugenden Schutz durch behördliche Vorabkontrollen und Genehmigungen. Selbstzertifizierung durch Hersteller und nachträgliche Schadenersatzansprüche reichen nicht aus.

Ressourcen für Vollzugsbehörden: Eine wirksame Marktaufsicht erfordert ausreichende Ressourcen. Das gilt natürlich auch im Bereich des Arbeitnehmer:innenschutzes (Arbeitsinspektorate)

Kollektive Rechtsdurchsetzung ermöglichen: Individuelle zivilrechtliche Klagen alleine schaffen kein Kräftegleichgewicht. Verbandsklagsbefugnisse für Organisationen, die Bürger- und Verbraucher:inneninteressen für Betroffene vertreten, sind deshalb notwendig.

Unabhängige Zertifizierung: Eine externe Zertifizierung von KI Systemen mit hohem Risiko wird aufgrund der VO wohl nur selten tatsächlich erfolgen. Einerseits, weil „Stand-alone"-Systeme mit hohem Risiko meist nur einer herstellerseitigen Prüfung zu unterziehen sind und andererseits, weil Systeme nach Annex II nur dann als KI mit hohem Risiko zu qualifizieren sind, wenn sie einer externen Zertifizierung unterliegen, was wiederum durch andere Produktstandardregeln festgelegt wird. Eine ex-ante Prüfung wird dabei nur selten verlangt. Bei hochriskanter KI müssten aus AK-Sicht aber ausnahmslos unabhängige, externe Prüfer:innen, herangezogen werden.

Zu den Konsument:innenanliegen im Detail

Anwendungsbereich (Art 2 Abs 1c)
Begrüßt wird, dass auch Hersteller und Nutzer:innen von KI-Systemen aus Drittstaaten vom Anwendungsbereich erfasst sind, sofern die KI-Ergebnisse in der EU genutzt werden. Zudem sollte aber auch in den Anwendungsbereich fallen, wenn EU-Bürger:innen von KI aus Drittstaaten betroffen sind.

Definitionen (Art 3)
Der Entwurf beinhaltet einige Definitionsdefizite. ZB. sind „**User**" definitionsgemäß nur **professionelle Anwender**. (Private) **Endnutzer:innen** von KI-Produkten und Diensten sind nicht erfasst. Schutznormen zu ihren Gunsten können somit nicht verankert werden können.

Darüber hinaus können Personen auch von KI betroffen sein, ohne direkt KI-Anwendungen zu nutzen (zB. als Subjekte der Überwachung). Bei automatisierten Einzelentscheidungen kann zwar auf die DSGVO verwiesen werden, aber der Begriff „**Betroffene**" geht darüber hinaus und sollte sich etwa auch auf eine KI-basierte Bildung von statistischen Gruppen erstrecken, da auch diese Folgen für Einzelpersonen haben können.

Ebenso erscheint die Definition von **„Sicherheitskomponenten eines Produktes oder Systems"** etwas willkürlich. Warum werden nur bestimmte Funktionen von KI hervorgestrichen, andere, ebenso riskante, aber nicht (zB. Spracherkennung, Biometrie bei Handys)?

Der Entwurf lässt auch eine prinzipielle kritische Distanzierung zu Technologien vermissen, die Menschenwürde berühren bzw. verletzen können, wie etwa „**Emotionserkennungssysteme**" oder die **biometrische Fernidentifikation von Personen**. Eine klare Abgrenzung zwischen KI, die grundsätzlich zum Einsatz kommen darf und solcher, der der Betrieb zu versagen ist, wäre wünschenswert.

Ziffer 44 fasst unter dem Begriff „**ernster Vorfall**" den Tod einer Person, ernste Gesundheitsfolgen oder Schäden am Eigentum, an der Umwelt oder kritischen Infrastrukturen zusammen. Bei der Umschreibung von hochriskanter KI (Artikel 6 ff) fehlen einige dieser Tatbestandselemente. Erwähnt werden nur Gefahren für Gesundheit und Sicherheit, dafür aber werden auch negative Folgen für die Grundrechte erwähnt. Die Risikoszenarien sollten durchgängig kohärent sein.

Verbotene Praktiken (Art 5)
KI-Systeme, die eine Bedrohung für die Sicherheit, Lebensgrundlagen und Rechte darstellen, sollen verboten sein. Doch im Entwurf wird dieses Prinzip oft durchlöchert. So sollen etwa **subliminare, verhaltensmanipulierende Techniken** verboten sein, allerdings nur dann, wenn sie den Betroffenen nicht bewusst sind und physischen bzw. psychischen Schaden anrichten. Von **wirtschaftlichem Schaden** ist nicht einmal die Rede. Ein Verbot von unbewusster Manipulation sollte allerdings nicht vom Eintritt eines Schadens abhängig sein. Schon gar nicht bei **Techniken, die die Verletzlichkeit bestimmter**

Personengruppen ausnützen. Solche Praktiken widersprechen per se schon der Menschenwürde und Persönlichkeitsrechten. Ebenso sind die Einschränkungen beim **„social scoring"** kritisch zu hinterfragen. Auch wenn die behördliche Bewertung von sozialem Verhalten verboten wird, so bleibt trotzdem vieles erlaubt. Ein Verbot soll nämlich nur für Daten gelten, die ursprünglich für andere Zwecke gesammelt wurden oder wenn die resultierenden Benachteiligungen unverhältnismäßig zum sozialen (Fehl-)Verhalten sind. Werden hingegen Daten von vornherein zum Zweck des Scorings erhoben, so bleibt die Bewertung von sozialem Verhalten erlaubt. Hier sollte es kaum Spielraum für zulässige Anwendungen geben. Benötigt wird ein generelles Verbot der sozialen Überwachung und Profilbildung der Bevölkerung. Unklar ist auch, was für social scoring gilt, das vom Verbot nicht erfasst und dennoch grundrechtswidrig ist. Können Praktiken, die nach Art 5 nicht untersagt sind, mit Blick auf die EMRK oder DSGVO verboten werden (etwa soziales Scoring durch die Privatwirtschaft)? Der Entwurf böte jedenfalls die Chance, auch Unzulänglichkeiten im Artikel 22 DSGVO zu beseitigen (Erweiterung des Schutzes auf statistische Gruppen ohne Personenbezug und auf Fälle mit abschließender menschlicher kontrollierender Aufsicht). Auch die Ausnahmen vom Verbot (Einwilligung, Rechtsakt, Vertragsnotwendigkeit) sind zu weitreichend und deshalb überarbeitungsbedürftig.

Ziffer d verbietet die biometrische Fernidentifikation von Personen in Echtzeit im öffentlichen Raum für Zwecke der Rechtsdurchsetzung. Auch hier gibt es umfangreiche Ausnahmen. Begrüßt wird, dass der Einsatz solcher Systeme in der Regel einer vorherigen Genehmigung durch die Justiz oder einer unabhängigen Verwaltungsbehörde bedarf. **Angemessen wäre allerdings auch hier ein weitgehend ausnahmsloses Verbot des Einsatzes KI-basierter biometrischer Erkennung von Personen ohne deren Zustimmung.**

Unvertretbar erscheint die Einschränkung auf Echtzeiterfassungen. Auch die biometrische Auswertung von Videomaterial kann in Grundrechte eingreifen. Arbeitspapiere der EU-Kommission enthielten noch ein mehrjähriges Verbot der KI-Analyse von biometrischen Merkmalen für private wie öffentliche Akteure. Es ist das falsche Signal, wenn die VO kein (temporäres) Einsatzverbot ausspricht. Neben Datenschutzbedenken besteht auch die Gefahr von falschen Ergebnissen aufgrund von Fehlerraten. Menschen geraten irrtümlich ins Visier, obwohl sie nichts verbrochen haben. Die zentralen Forderungen der AK sind im Policy Brief "The body as an access key? Biometric methods for consumers" abrufbar.

Klassifizierung von KI-Systemen als hochriskant (Art 6)
Hochriskant sind KI-Systeme nur dann, wenn sie als Sicherheitskomponente oder –produkt nach den in Anhang II angeführten Harmonisierungsrechtsvorschriften gelten und einer Konformitätsbewertung durch Dritte unterzogen werden.

Für die Qualifizierung eines KI-Sicherheitsproduktes als hochriskant kann aber nicht ernsthaft ausschlaggebend sein, ob sie extern zu zertifizieren sind (was im Übrigen selten der Fall ist). Dieser Ansatz muss durch sachgerechte Kriterien ersetzt werden.

Als hochriskant gelten zudem die im Annex III aufgezählten Anwendungen. Diese Liste sollte nur deskriptiv sein, denn wichtige Bereiche finden gar keine Erwähnung (zB. KI, die sensible Gesundheitsdaten benutzt). Die EU-Kommission kann zwar den Annex III ergänzen, allerdings nur innerhalb der bereits angelegten Kategorien. Neue Kategorien sind ausgeschlossen. Damit können wichtige, verbraucher:innenrelevante Bereiche nicht erfasst werden. Zudem muss von weiteren Beispielen ein hohes Risiko in Form von Schäden an Gesundheit oder Sicherheit oder eine negative Beeinträchtigung von Grundrechten ausgehen. Wirtschaftliche Schäden sind nicht erwähnt.

Zusätzliche Anmerkungen zum Annex sind hier abrufbar: https://wien.arbeiterkammer.at/kuenstliche-intelligenz

Transparenz und Bereitstellung von Informationen für Nutzer (Art 13)
Es ist unakzeptabel, dass nur professionellen Anwendern Informationen zum KI-Betrieb zugänglich sein müssen. Auch Betroffene haben einen Anspruch auf Transparenz. Die in Abs 3 genannten Informationen müssen daher auch den von der Anwendung Betroffenen zugänglich sein.

Menschliche Aufsicht (Art 14)
Die Anforderung einer menschlichen Aufsicht wird begrüßt. Unklar ist, welche Qualitätsanforderungen dabei einzuhalten sind und in welchem Verhältnis diese Anforderung zu Artikel 22 DSGVO steht, der automatisierte Einzelentscheidungen grundsätzlich auch ohne menschliche Aufsicht gestattet, im Gegenzug aber gewisse Rechte einräumt (zB. Anfechtung).

Qualitätsmanagement (Art 17)
Provider sind zu einer Strategie ua. für die rechtliche Konformität verpflichtet. Es sollte klargestellt werden, dass dies auch die Einhaltung datenschutzrechtlicher

Bestimmungen umfasst. Abzulehnen ist, dass sich diese Verpflichtungen nach der Größe des Unternehmens richten. Risiken müssen unabhängig von der Unternehmensgröße minimiert werden.

Aussetzung der Konformitätsbewertung (Art 47)
Marktüberwachungsbehörden sollen Verfahren zur Konformitätsbewertung in bestimmten Fällen aussetzen können. Die dafür ausschlaggebenden „außergewöhnlichen Gründe" sind viel zu unbestimmt.

Transparenzpflichten für bestimmte AI-Systeme (Art 52)
Informationspflichten beim Einsatz von Chatbots sind grundsätzlich zu begrüßen. Die Bestimmung ist jedoch um generelle vorherige Informations- und nachträgliche Auskunftsrechte für alle von KI betroffenen Personen zu erweitern. Emotionserkennungssysteme greifen erheblich in die Grundrechte ein – eine bloße Kenntlichmachung ist kein hinreichender Schutz. Ihr Einsatz sollte grundsätzlich zu den verbotenen Praktiken des Artikel 5 zählen.

Weiterverarbeitung personenbezogener Daten in KI-„Sandboxes/Reallaboren" (Art 54)
Personenbezogene Daten, die für andere Zwecke erhoben wurden, sollen zum Testen benutzt werden dürfen, wenn ein erhebliches öffentliches Interesse besteht und anonyme Daten nicht ausreichen. Dies höhlt jedoch die DSGVO aus, die einer Weiterverarbeitung von Daten zu anderen Zwecken enge Grenzen setzt. Betroffene wären von einem solchen Vorhaben zu informieren und ihre Zustimmung einzuholen. Eine Missachtung des Selbstbestimmungsrechtes über eigene Daten wäre in hohem Maße grundrechtswidrig.
Zudem ist zu überwachen, ob während des Testens hohe Grundrechtsrisiken bestehen. Auch diesem Risiko kann man Personen nicht zu Testzwecken ungefragt aussetzen. Es braucht eine explizite Zustimmung und Datenschutzbehörden sollten ein solches Vorhaben vorab prüfen und geeignete Auflagen erteilen (bzw. untersagen) können.

Weitere Verbraucher:innenanliegen und detaillierte Informationen sind in der Analyse des VO-Entwurfes Künstlicher Intelligenz aus Verbraucher:innensicht unter der Web-Adresse https://wien.arbeiterkammer.at/kuenstliche-intelligenz abrufbar.

3. Fazit

Mit dem Weißbuch hat die Kommission einen Plan zur Diskussion gestellt, wie zukünftig mit Künstlicher Intelligenz zu verfahren ist. Darin wurde lobenswerterweise stets ein „menschenzentrierter Ansatz" und die Einbindung aller Stakeholder:innen propagiert. Es ist prinzipiell zu begrüßen, dass KI ein europäischer Rechtsrahmen gegeben werden soll. Doch der vorliegende Verordnungsentwurf enttäuscht auf vielen Ebenen und beschränkt sich auf eine sehr technikzentrierte Sicht. Viele notwendige Rahmenbedingungen für Arbeitnehmer:innen und Konsument:innen finden keine Erwähnung. Der „menschenzentrierte Ansatz" bleibt zugunsten eines liberalen Marktes für KI auf der Strecke.

Europa sollte eine Führungsrolle übernehmen und alle Interessen zum gemeinsamen Nutzen berücksichtigen. Dazu bedarf es allerdings der Ergänzung und Präzisierung des geplanten Rechtsrahmens um hohe Sicherheitsstandards und einen hohen Grundrechtsschutz aufrechtzuerhalten.

Die wichtigsten Eckpunkte wären dabei:

- **Regeln nicht ausschließlich für Hochrisiko Anwendungen**: Auch weniger risikobehaftete KI bedarf eines Regelwerks

- **Mitbestimmung**:
  Die Einbindung Betroffener ist essenziell. Insbesondere beim Einsatz von KI im Arbeitsumfeld ist ein hohes Maß an betrieblicher und überbetrieblicher Mitbestimmung durch Arbeitnehmer:innen und ihrer Vertretungen notwendig. Sowohl im laufenden Betrieb als auch bei der Einführung solcher Anwendungen sollten Mitarbeiter:innen bzw. ihre Interessensvertretungen umfangreich eingebunden sein. Die Einführung von KI-Systemen in Produktions- und Organisationsabläufen kann auch wesentlich zielgerichteter und besser gestaltet werden, wenn Arbeitnehmer:innen und ihre Vertretungen frühzeitig eingebunden werden und Projekte mitgestalten können. Dies sollte aktiv gefördert werden.

- **KI im Arbeitszusammenhang sollte prinzipiell als Hochrisiko-Anwendung gelten**

- **Rechte und Pflichten klar verankern:**
  Beschwerdemöglichkeiten bei unabhängigen Stellen, Informationspflichten und Selbstbestimmungsmöglichkeiten der Betroffenen

sind essenziell zur Abwendung und Ausgleich von Schäden, Schutz vor Eingriffen in Grund- und Persönlichkeitsrechte sowie für ein hohes Datenschutzniveau. Klare Haftungs- und Versicherungsregelungen müssen verankert werden.

- **Keine umfassende Selbstzertifizierung**: Kontrolle, Konformitätsbewertungen und Zertifizierungen sollten nicht den Herstellern selbst überlassen werden, sondern vorrangig durch unabhängige Stellen erfolgen.

- **Überprüfbarkeit von KI-Entscheidungen herstellen**: KI ähnelt oft einer Blackbox. Eine höchstmögliche Überprüfbarkeit muss aber stets gegeben sein. Der Mensch sollte immer die Kontrolle behalten.

- **Ausnahmen hintanhalten:**
Viele (begrüßenswerte) Ziele und Grundsätze werden in der VO durch zahlreiche Ausnahmen durchlöchert. In der Praxis bleibt oft vom Bekenntnis zu einem umfassenden Schutz von Grundrechten, Datenschutz, Arbeitnehmer:innen-Schutz, dem Schutz der Privatsphäre und ähnlichem wenig übrig. Grundsätzlich verbotene Praktiken wirken stark aufgeweicht, notwendige Teilbereiche werden nicht abgedeckt.

- **Effektiver Rechtsschutz**:
Rechtsschutzmöglichkeiten für Einzelne aber auch kollektive Interessensvertretungen (Verbandsklagen) müssen umfassend zugänglich sein. Auf eine ausreichende Ressourcenausstattung der Vollzugs- bzw. Kontrollbehörden (inklusive DSB, Arbeitsinspektorate) ist zu achten.

- **Aus- und Weiterbildung**:
KI am Arbeitsplatz bedarf einer Verpflichtung zu vorbeugenden Maßnahmen wie Aus- und Weiterbildung. Das schützt Arbeitnehmer:innen und versetzt sie in die Lage, die Rolle von Daten und KI, sowie ihren Einfluss auf Arbeitsorganisation zu verstehen. Prävention und das Vorsorgeprinzip müssen Teil des regulatorischen Rahmenwerks sein.

- **Ungewünschte Anwendungen verbieten**:
KI eröffnet viele Möglichkeiten. Doch anfallende Daten können mittels Algorithmen auch benutzt werden um Betroffene zu überwachen, zu kontrollieren, zu bewerten und sie zu identifizieren (auch aus anonymisierten Daten). Sowohl im Arbeitszusammenhang, als auch bei Konsument:innen bedarf es deshalb strenger Regelungen und Mitbestimmungsmöglichkeiten. **Bestimmte Anwendungen sollten dabei gänzlich verboten sein**.

- **Arbeitnehmer:innenschutz und Inklusion**
Der Sicherheit und Gesundheit am Arbeitsplatz muss ein wichtiger Stellenwert eingeräumt werden. Schutz vor körperlichen und psychischen Risiken ist für Arbeitnehmer:innen wichtig. Gerade im Hinblick auf Arbeitsunfälle und arbeitsbedingte Erkrankungen bedarf es ausreichender Kontrollmöglichkeiten und der unabhängigen Zertifizierung von Systemen. Reine Selbstkontrolle führt oft zu lückenhafter Sicherheit, Arbeitsunfällen und Berufskrankheiten. Deren Folgen werden externalisiert und die Kosten den Sozialversicherungen sowie den betroffenen Arbeitnehmer:innen aufgebürdet. Unternehmen haben zudem ein Interesse daran, ein „Minimum Viable Product“ auf den Markt zu bringen, um Entwicklungskosten gering zu halten. Arbeitnehmer:innenschutz braucht aber höchstmöglich sichere Maschinen oder Technologien. In diesem Spannungsfeld ist die EU gefragt, Arbeitnehmer:innen zu schützen. Ebenso fehlt auch eine stärkere Berücksichtigung von Menschen mit Behinderungen (zB. Hör- und Sehdefizite).

- **Entwicklungs- und Anpassungsmöglichkeiten der VO schaffen**:
Die Taxonomie der Anwendungen im Anhang wird sehr starr definiert. Angesichts der Dynamik des technischen Fortschritts und neuer Anwendungsfelder für KI, sollte hier mehr Raum für Adaptierungen gelassen werden, um auf zukünftige Probleme und Herausforderungen reagieren zu können.

Kontaktieren Sie uns!

In Wien:

Mathias Grandosek
T +43 (1) 501 65 12389
mathias.grandosek@akwien.at

Fridolin Herkommer
T +43 (1) 501 65 12883
fridolin.herkommer@akwien.at

Daniela Zimmer
T +43 (1) 501 65 12722
daniela.zimmer@akwien.at

Martina Chlestil
T +43 (1) 501 65 12729
martina.chlestil@akwien.at

Michael Heiling
T +43 (1) 501 65 12665
michael.heiling@akwien.at

Julia Nedjelik-Lischka
T +43 (1) 501 65 12205
julia.nedjelik@akwien.at

Bundesarbeitskammer Österreich
Prinz-Eugen-Straße 20-22
1040 Wien, Österreich
T +43 (0) 1 501 65-0

www.arbeiterkammer.at

In Brüssel:

Alice Wagner
T +32 (2) 230 62 54
alice.wagner@akeuropa.eu

AK EUROPA
Ständige Vertretung Österreichs bei der EU
Avenue de Cortenbergh 30
1040 Brüssel, Belgien
T +32 (0) 2 230 62 54
www.akeuropa.eu

Über uns

Die Bundesarbeitskammer (AK) ist die gesetzliche Interessenvertretung von rund 3,8 Millionen ArbeitnehmerInnen und KonsumentInnen in Österreich. Sie vertritt ihre Mitglieder in allen sozial-, bildungs-, wirtschafts- und verbraucherpolitischen Angelegenheiten auf nationaler sowie auch auf der Brüsseler EU-Ebene. Darüber hinaus ist die Bundesarbeitskammer Teil der österreichischen Sozialpartnerschaft. Die AK ist im EU-Transparenzregister unter der Nummer 23869471911-54 registriert.

Die Aufgaben des 1991 eröffneten AK EUROPA Büros in Brüssel sind einerseits die Repräsentation der AK gegenüber europäischen Institutionen und Interessensorganisationen, das Monitoring von EU-Aktivitäten und die Wissensweitergabe von Brüssel nach Österreich, sowie gemeinsam mit den Länderkammern erarbeitete Expertise und Standpunkte der Arbeiterkammer in Brüssel zu lobbyieren.