BUNDESARBEITSKAMMER

PRINZ-EUGEN-STRASSE 20-22
1040 WIEN
www.arbeiterkammer.at

Positionspapier der Bundesarbeitskammer

zum EU-Verordnungsentwurf „Künstliche Intelligenz“

Worum geht es inhaltlich und im Prozess

Der 2018 entstandene koordinierte Plan zur Entwicklung, Einsatz und Regulierung künstlicher Intelligenz (KI) sieht vor, dass die Mitgliedstaaten der Europäische Union Strategien entwickeln, um eine Führungsrolle rund um vertrauenswürdige künstliche Intelligenz im globalen Wettbewerb übernehmen zu können. 2020 entstand dazu das Weißbuch, welches einen risikobasierten Ansatz zur Regulierung von KI vorsieht. 2021 liegt nun ein Verordnungsentwurf der Europäischen Kommission vor.

Was ist gut an dem derzeitigen Entwurf?

Zu begrüßen ist, dass ein breit angelegter Prozess, dieses zukunftsweisende Thema aufgreift und versucht, einen Rahmen zu Förderung, Entwicklung und Einsatz, sowie zur Regulierung zu schaffen. Es wurde dabei ein risikobasierter Ansatz gewählt, der unabhängig von der Technologie die Auswirkungen betrachtet und versucht das dabei entstehende oder entstandene Risiko zu bewerten woraus sich wiederum der Grad des Regulierungserfordernisses ableiten soll. Die Risikokategorien umfassen unakzeptables, hohes, limitiertes und geringes Risiko. Ein Annex (2 und 3) listet Beispiele von Anwendungen je Risikokategorie auf. Spätestens hierin ergeben sich jedoch eine Reihe von Fragestellungen, denn die Risikoeinstufung ist entscheidend für die Gültigkeit von Regulierungsbestimmungen.

Welche Kritik ist angebracht, was fehlt?

Der Entwurf hat einen sehr technikzentrierten Fokus mit Blick auf die Erfordernisse des Binnenmarkts. Der ursprünglich propagierte „menschenzentrierte Ansatz“ findet sich kaum wieder. Wichtige Schutzmechanismen für ArbeitnehmerInnen und KonsumentInnen fehlen, Möglichkeiten zur Mitbestimmung ebenso. Viele im Grunde richtige Ansatzpunkte werden durch Ausnahmen und Einschränkungen stark verwässert.
Inwiefern bedeutet der Annex eine abschließende Taxonomie, wie kann diese laufend aktualisiert werden und was ist, wenn sich die Risikoauswirkung einer Technologie verändert? Wie kann die Taxonomie laufend und der technischen Entwicklung entsprechend aktualisiert werden? Wie wird künstliche Intelligenz überhaupt definiert, sprich, was gilt es überhaupt in die Taxonomie aufzunehmen? Auch das institutionelle Setting der mit der Regulierung beauftragten Behörde(n) ist offen und entscheidend für den Umgang mit den Entwicklungen künstlicher Intelligenz und ihren Risiken.

Was braucht es daher:

- KI-Anwendungen, die ArbeitnehmerInnenrechte, Arbeitsbedingungen und die Gesundheit am Arbeitsplatz berühren sollten prinzipiell als hochriskant eingestuft werden und einer entsprechenden Regulierung unterliegen. Bestimmte – für ArbeitnehmerInnen besonders riskante – Anwendungen sollten nicht erlaubt sein
- Das Prinzip der menschlichen Kontrolle soll ArbeitnehmerInnen und ManagerInnen gleichermaßen umfassen.
- Transparenzbestimmungen sollen auch den Bildungsaspekt abdecken, sodass KI-Anwendungen verstanden und ihre Funktionsweisen erlernt werden können.
- Stärkung von ArbeitnehmerInnenbeteiligung 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 für ArbeitnehmerInnen-Management von autorisierten Stellen nötig sowie ein Mechanismus, der Ex-Ante Compliance und Ex-Post Enforcement kombiniert. Die Normung zeigt ein demokratisches Defizit– die Beteiligung der Gewerkschaften ist nötig.

- Begleitende Aus- und Weiterbildungen für die betrieblichen InteressenvertreterInnen und alle ArbeitnehmerInnen.
- Neue Anwendungen bergen unbekannte Risiken, das Vorsichtsprinzip ist anzuwenden. Arbeitsunfällen und arbeitsbedingten Erkrankungen muss vorgebeugt werden und ArbeitnehmerInnen mit speziellen Bedürfnissen müssen mitbedacht werden. Die Arbeitsinspektion als Aufsichtsbehörde braucht daher ausreichend personelle und technische Mittel, um die neuen Aufgaben abzudecken.
- Grund- und Persönlichkeitsrechte, Datenschutz, ArbeitnehmerInnenschutz und KonsumentInnenrechte müssen Priorität haben und dürfen nicht durch Ausnahmen und Einschränkungen ausgehöhlt werden.

I. KI und Arbeitswelt

Allgemein: Vollständiges Fehlen des im Weißbuch angekündigten „menschenzentrierten Konzepts".

Mit ihrem ***Vorschlag für einen Rechtsrahmen zur Künstlichen Intelligenz*** strebt die Kommission selbst folgende Ziele an: Es muss gewährleistet sein, dass die auf dem Unionsmarkt in Verkehr gebrachten und verwendeten KI-Systeme sicher sind und die **bestehenden Grundrechte und die Werte** der Union wahren. Zur Förderung von Investitionen in KI und Innovationen muss **Rechtssicherheit** gewährleistet sein. Governance und die wirksame Rechtsdurchsetzung zur Wahrung der Grundrechte sowie Sicherheitsanforderungen an KI-Systeme müssen gestärkt und die Entwicklung eines Binnenmarkts für rechtskonforme, sichere **und vertrauenswürdige KI-Anwendungen** muss erleichtert werden.
Noch in ihrer ***Mitteilung vom 25.4.2018*** 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 angesichts des Ausmaßes der mit KI verbundenen Herausforderungen ein breites Spektrum von TeilnehmerInnen (ua Gewerkschaften) zu mobilisieren sind, um an **allen Aspekten** von KI zu arbeiten. **Die BAK weist besorgt 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 die betroffenen ArbeitnehmerInnen bei der Anwendung von KI am Arbeitsplatz!**
Auch vor dem Hintergrund, dass die Europäische Kommission in ihrem ***Weißbuch*** ein „menschenzentriertes KI-Konzept" für den Arbeitsplatz unter Einbeziehung der Sozialpartner angekündigt hat, **ist es umso bedenklicher und enttäuschender, dass in der Verordnung im Wesentlichen ein rein technikzentrierter Ansatz gewählt wurde**. ArbeitnehmerInnen und deren (betriebliche) Interessenvertretungen kommen dort als eigene Kategorien schlichtweg nicht vor. Im Weißbuch wurden wesentliche Gefahren, wie die Gefahr der Überwachung von ArbeitnehmerInnen, oder die Gefahr diskriminierender KI, dargestellt. Dies wurde von der BAK 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 umfassender Einbeziehung von ArbeitnehmerInnen und ihrer Interessenvertretungen) gleichgewichtig das Ziel haben, Arbeit besser und humaner zu gestalten.** Es darf nicht alles zugelassen werden, was auch 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**. **Den ArbeitnehmerInnen und ihren Interessenvertretungen müssen immer auch entsprechende Mitsprache- und Vetorechte zukommen**.

- Die noch im Weißbuch an mehreren Stellen angeführten Sozialpartner sollen etwa nach dem Willen der Kommission im Europäischen Ausschuss für Künstliche Intelligenz nicht vertreten sein.

  Für einen „menschenzentrierten" KI-Ansatz, der auch die Auswirkungen der KI-Anwendungen auf die Arbeitswelt und ArbeitnehmerInnen im Blickpunkt hat, wäre es unabdingbar, **dass auch die Interessenvertretungen von ArbeitnehmerInnen und nicht nur die nationalen Behörden in den beratenden Gremien der Kommission vertreten sind.**

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 ArbeitnehmerInnen haben.** Diese Themen der Arbeitswelt und der Mitbestimmung – im Sinne eines umfangreichen europäischen und nationalen Ansatzes unter Einbeziehung der wichtigsten Stakeholder – werden in der Verordnung nicht einmal im Ansatz erwähnt. **Die wichtige Rolle der betrieblichen und überbetrieblichen ArbeitnehmerInneninteressenvertretung bei der Einführung/Verwendung von KI am Arbeitsplatz, um das dort herrschende Machtungleichgewicht zwischen ArbeitgeberInnen und ArbeitnehmerInnen auszugleichen, gilt es explizit zu verankern!**
- Im Weißbuch kam die Kategorie der Arbeit und der ArbeitnehmerInnen noch in Ansätzen vor, auch sprach die Europäische Kommission von einem „**menschenzentrierten" KI-Ansatz** am Arbeitsplatz und wies auf die Gefahr der Überwachung von ArbeitnehmerInnen durch KI sowie durch diskriminierende KI und auch auf die Kompetenzanforderungen für ArbeitnehmerInnen 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 verwendet werden sollen, 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 oder zu verbieten, die sich durch die vielfältigen Einsatzmöglichkeiten von KI-Anwendungen im Beschäftigungsverhältnis und aufgrund des dort herrschenden Machtungleichgewichts zwischen ArbeitgeberInnen und ArbeitnehmerInnen ergeben.** Augenscheinlich orientiert sich diese Verordnung primär an Technologieanbietern, wobei doch der Schutz der EU-BürgerInnen und der ArbeitnehmerInnen vorrangig sein müsste.
- Zum Schutz von ArbeitnehmerInnen dürfen **bestimmte KI-Anwendungen in der Arbeitswelt gar nicht erst zugelassen** werden. **Anwendungen, die auf die Arbeitsrealitäten und Arbeitsbedingungen Auswirkungen haben, sind als „hochriskant" zu klassifizieren**. Insbesondere darf die vorzunehmende Konformitätsbewertung nicht ohne Einbeziehung der Betroffenen, dh der ArbeitnehmerInnen und ihrer Interessenvertretungen, erfolgen. **Bei der Einführung derartiger KI-Systeme am Arbeitsplatz sollte jede Bewertung von Risiken in Abstimmung mit den Interessenvertretungen der ArbeitnehmerInnen erfolgen. Werden die Risiken als zu hoch eingestuft, müssen diese von den AnbieterInnen 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 jedermann Anspruch auf Geheimhaltung seiner 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 aber 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 die ArbeitnehmerInnen 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, die also anonymisiert wurden. Bezüglich letzteren räumen ExpertInnen allerdings ein, dass Algorithmen durch maschinelles Lernen so gut wie jede Anonymisierung rückführen können und ArbeitnehmerInnen re-identifizierbar werden. Profiling, Scoring und Verhaltensprognosen sowie automatisierte Entscheidungsfindungen mit Hilfe von Algorithmen, maschinellem Lernen und KI können ArbeitnehmerInneninteressen jedenfalls massiv gefährden. ArbeitnehmerInnenverhalten, persönliche Eigenschaften uvm 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.

- ArbeitnehmerInnen fürchten um die Wertschätzung für ihre menschliche Arbeit: Werden ArbeitnehmerInnen noch als individuelle Personen wahrgenommen oder wird menschliche Arbeit zukünftig immer mehr wie automatisierte und (leicht) automatisierbare Prozesse definiert und bewertet? 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 ArbeitnehmerInnen wird zunehmend in Zahlen ausgedrückt, gemessen, verglichen, analysiert und es werden daraus automatisiert Entscheidungen und Vorhersagen getroffen. Der Mensch am Arbeitsplatz wird zu einem bloßen messbaren Produktions- und Kostenfaktor herabgewürdigt; der immaterielle Wert der Arbeit und die Würde der Arbeitenden bleiben dabei auf der Strecke. Die Wahrung der Menschenwürde, die 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 keineswegs dem angekündigten „menschenzentrierten Ansatz“. Deshalb sollen hier noch einmal die grundlegenden Herausforderungen dargelegt werden, an **denen sich die Regeln für Anwendungen in der Arbeitswelt orientieren sollten**. Diese legen auch **Gründe dar, warum es für die Arbeitswelt einen wirklich „menschenzentrierten“ Ansatz braucht, der auf die bessere und humane Gestaltung der Arbeit und nicht nur auf die Gestaltung der Technik abzielt**:

- KI wird die Arbeitsbedingungen einschneidend verändern, erste Anzeichen sind bereits erkennbar (zB Einsatz von Bewerbungs- oder Karrieretools, automatisierte Prämienberechnungen, usw). Die wirtschaftlichen Chancen, die sich durch den Einsatz von KI ergeben, sind zu nutzen, aber – aufgrund der Tatsache, dass damit auch die technischen Möglichkeiten der **Überwachung am Arbeitsplatz** und der Verwendung von ArbeitnehmerInnendaten zunehmen – müssen **die Rechte der Beschäftigten durch konkrete Regelungen geschützt werden!**
- IT/KI-Systeme (Laptop, Smartphone, vernetzte Maschinen und Arbeitsmittel, Programme zur Personalverwaltung und Betriebsorganisation) werden immer vielfältiger und komplexer.

Die Menge der dabei generierten und verwendbaren Beschäftigtendaten nimmt exponentiell zu und auch die technischen Verknüpfungs- und Analyse-Möglichkeiten dieser Daten werden immer ausgereifter und aussagekräftiger – bis hin zum Erstellen von Bewertungen und Verhaltensvorhersagen von ArbeitnehmerInnen (Profiling) und automatisierter Entscheidungsfindungen im Bereich der Personalverwaltung, der Personal- und Karriereplanung, des Einsatzes von Personalinformationssystemen etc.

- **Entscheidend für den Schutz von ArbeitnehmerInnen 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 dem Arbeitgeber – von betrieblichen und überbetrieblichen Interessenvertretungen sein.
- Hervorgehoben sei auch, dass **eine allfällige Zustimmung der ArbeitnehmerInnen zur Verwendung ihrer personenbezogenen Daten in der Regel nicht freiwillig erfolgen kann, weil sich im Arbeitsverhältnis keine gleichberechtigten VertragspartnerInnen gegenüberstehen**. So zeigt die Praxis, dass ArbeitnehmerInnen im aufrechten Arbeitsverhältnis ihre Rechte so gut wie nie einfordern, also die Möglichkeit eine Beschwerde bei der Datenschutzbehörde bzw eine Klage bei Gericht einzubringen, nicht in Anspruch nehmen. 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 nur mangelhaft und meist in einer nicht leicht verständlichen Sprache, womit Transparenz, Information und Nachvollziehbarkeit bei den ArbeitnehmerInnen und ihrer Interessenvertretungen in der Praxis in den seltensten Fällen ausreichend gegeben ist** (so erfolgt die Befragung der betroffenen ArbeitnehmerInnen und ihrer Interessenvertretungen bei der Datenschutz-Folgenabschätzung nach der DSGVO oft nur ungenügend oder unterbleibt sogar ganz).

- Um die positiven Potenziale von KI auch für ArbeitnehmerInnen zu heben und sie dennoch vor den 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 die arbeitenden Menschen und die 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 und oft schnelllebigen Umsetzung auch die entsprechende Position der ArbeitnehmerInnenvertretung und damit der ArbeitnehmerInnenrechte gewährleistet werden kann.

II. KI und KonsumentInnen

Die Absicherung eines hohen Verbraucherschutzniveaus ist auch bei Algorithmen und KI wichtig. **KonsumentInnen müssen vor einer Aushöhlung ihrer Grund- und Freiheitsrechte, Intransparenz, Diskriminierung, körperlichen sowie psychischen Risken und sonstigen Schadensrisiken, die von derartiger Analysesoftware ausgehen,** bestmöglich geschützt werden.

Um KonsumentInnen angemessen zu schützen, sind folgende Punkte erforderlich

- **Regeln nicht nur für Hochrisiko-KI**. Freiwillige Selbstverpflichtungen sind zu wenig. Auch bei „bloß“ riskanten Anwendungen sind Transparenz, Diskriminierungsfreiheit, Beschwerderechte durch Vorschriften abzusichern
- **Verankerung von Rechten für betroffene BürgerInnen und VerbraucherInnen**: ua das Recht auf Information, Auskunft, Selbstbestimmung (Möglichkeit, KI-Analysen und Entscheidungen basierend auf persönlichen Daten auch abzulehnen), Beschwerderechte.
- **Verbot von gesellschaftlich unerwünschten KI-Systemen** statt lückenhafte Verbote einiger Spielarten von Social Scoring, biometrischer Fernüberwachung und Verhaltensmanipulation.
- **Konkrete Benennung von Risiken, die Hersteller und Nutzer ausschließen bzw minimieren müssen:** 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** (bzw ihnen zurechenbarer Dienstleister) statt bloßer Selbstzertifizierung durch die Hersteller.
- **KI-Entscheidungen, -Dienste und –Produkte müssen – bei sonstigem Verbot – tatsächlich erklär- und überprüfbar bleiben**, vor allem in Hinblick auf unzulässige Diskriminierung, Benachteiligung, Verhaltensmanipulation oder Betrügereien.
- **Schutznormen für biometrische KI-Analysen bei Verbrauchergeschäften.**
- **keine Ausnahmen von der DSGVO für den Dateneinsatz in KI- „Reallaboren“**
- **institutionelle Einbindung der Betroffenen** bei interessensabwägenden Entscheidungen über die (Un-)Zulässigkeit von konkreten KI-Anwendungen.
- **Überarbeitung der unzeitgemäßen Regeln für Produkthaftung und Produktsicherheit** um sie „KI-fit“ zu machen
- **kollektive Rechtsschutzmöglichkeiten für Betroffene ua durch Verbandsklagbefugnisse.**

Allgemeine konsumentenpolitische Defizite des Entwurfes:

Verbraucheranliegen werden überhaupt nicht mitgedacht: KonsumentInnen werden durch Algorithmen oft kategorisiert und bewertet. Die EU-Kommission bagatellisiert die Risiken, wenn sie dafür nur eine freiwillige Selbstverpflichtung empfiehlt. 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. Die BAK hält deshalb gesetzliche Anforderungen nicht nur für Hochrisiko-KI, sondern für alle KI-Anwendungen für angemessen. Diese sollten entsprechend ihrer Gefahrenneigung abgestuft sein.

„KI muss vertrauenswürdig sein!“: Auch die EU Kommission sieht bei KI viele Bedrohungsszenarien. Die vorgesehenen Rechtsinstrumente sind aber schwach. Für Entwickler und Verwender sollen laut Kommission keine „unverhältnismäßig hohen Bürden“ entstehen. Man setzt primär auf die Regulierung von hochriskanter KI. Es ist jedoch irrelevant, ob ein Schaden von einer hochriskanten oder bloß risikobehafteten KI herrührt. Vorabkontrolle, Transparenz – und Beschwerderechte sind deshalb in jedem Fall notwendig.

Skepsis gegenüber „ethischer“ Technik angebracht: Der Philosoph Richard David Precht spricht vom „Irrsinn, Maschinen Ethik einzuprogrammieren“: „Künstliche Intelligenz etwa darauf zu programmieren, wie sie sich in ethischen Grenzfällen verhalten soll“ sei „ein Angriff auf die Menschenwürde“.

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: die im Entwurf beinhalteten Verbote greifen nur in wenigen spezifischen Fällen. Klare Grenzen und rote Linien werden nicht gesetzt: keine Definition maximal zulässiger Restrisiken; kein Verbot von Diskriminierungsrisiken; Selbstzertifizierung der Hersteller ohne klare Vorgaben. Man überlässt vieles nur Herstellern und allenfalls noch nachprüfenden Behörden. Was fehlt sind Verbote ohne vielfältige Ausnahmen, Risikobenennung (auch bei Diskriminierungsgefahren), Selbstbestimmungsrechte darüber, ob KI die eigene Person betreffende Entscheidungen überhaupt treffen darf, Informationspflichten, behördliche Vorabprüfung der Folgen für Menschenwürde und Freiheitsrechte, Produktsicherheit und –haftung, außergerichtliche Beschwerdestellen und Verbandsklagsbefugnisse im Interesse aller Betroffenen.
Der bloßer Verweis auf die in Art 22 DSGVO enthaltenen Rechte reicht dabei keinesfalls aus (siehe AK-Stellungnahme zur Evaluation der Datenschutz-Grundverordnung).

Blackbox auch für die Verantwortlichen:
KI ähnelt einer Blackbox. Auch KI-ExpertInnen können bei selbstlernender Software oft nicht genau erklären, warum eine KI zu bestimmten Ergebnissen gelangt. Können Hersteller und Nutzer KI-Ergebnisse aber nicht verantworten, weil sie sie selbst nicht begreifen und beherrschen können, ist aus Sicht der BAK eine Anwendung zu verbieten.

Transparenz? Nicht für BürgerInnen und VerbraucherInnen:
Transparenzverpflichtungen für „User“ gelten nur für professionelle Anwender von KI Systemen. Gegenüber betroffenen EndnutzerInnen und KonsumentInnen 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, und sich im Bedarfsfall nicht wehren. 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, insbesondere bei grenzüberschreitenden Problemen:
Zulassungen und Konformitätsentscheidungen eines Mitgliedsstaates sind in der gesamten EU wirksam, was zu Problemen führen kann, wenn etwa die Niederlassungsstaaten von Herstellern, Nutzern und VerbraucherInnen auseinanderfallen. Es braucht deshalb niedrigschwellige Rechtsschutzmechanismen für Betroffene, um grenzüberschreitende Informationen einfordern oder Beschwerden tätigen zu können.

Mehr Prävention:
KonsumentInnen und ArbeitnehmerInnen erwarten sich einen vorbeugenden Schutz durch behördliche Vorabkontrollen und Genehmigungen. Selbstzertifizierung durch Hersteller von KI und nachträgliche Schadenersatzansprüche reichen nicht aus.

Ohne bestausgestattete Vollzugsbehörden kein Durchblick:
Eine wirksame Marktaufsicht erfordert ausreichende Ressourcen. Behörden können die komplexen Prüfaufgaben ansonsten weder finanziell noch fachlich bewältigen. Das gilt natürlich auch im Bereich des ArbeitnehmerInnenschutzes (Arbeitsinspektorate).

Kollektive Rechtsdurchsetzung ermöglichen (Beschwerden bei Behörden, Verbandsklagen):
individuelle zivilrechtliche Klagen alleine schaffen kein Kräftegleichgewicht. Verbandsklagsbefugnisse für Organisationen, die Bürger- und Verbraucherinteressen für Betroffene vertreten, sind deshalb auch im Bereich von KI-Anwendungen 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 BAK-Sicht aber ausnahmslos unabhängige, externe Prüfer, herangezogen werden.

Zu den Konsumentenanliegen im Detail:

Anwendungsbereich (Art 2 Abs 1 c)
Begrüßt wird, dass auch Hersteller und Nutzer 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-BürgerInnen von KI aus Drittstaaten betroffen sind.

Definitionen (Art 3)
Die augenfälligen Definitionsdefizite verweisen auf eine Regelungslücke im gesamten Entwurf: Auf von KI betroffene KonsumentInnen und ihren Schutzbedarf wird überhaupt nicht eingegangen. ZB sind **„User"** definitionsgemäß nur die **professionellen Anwender** von KI. (Private) **Endnutzer** von KI-Produkten und Diensten sind nicht erfasst. Sie sind in den Adressatenkreis unbedingt aufzunehmen, damit auch Schutznormen zu ihren Gunsten 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 hier noch darüber hinaus und sollte sich etwa auch auf eine KI-basierte Bildung von statistischen Gruppen erstrecken, da auch diese Folgen für die Einzelperson haben können.

Ebenso erscheint die Definition von **„Sicherheitskomponenten eines Produktes oder Systems"** etwas willkürlich**.** Es wird nicht erklärt, warum nur bestimmte Funktionen von KI hervorgestrichen werden, 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 (von wenigen Ausnahmen abgesehen) 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 Tatbestandelemente. 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)
Bei der Präsentation des Entwurfes nahm die EU-Kommission eine strikte Haltung in Bezug auf „unannehmbare Risiken" ein.

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, 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 menschlichen Verhaltens sollte allerdings nicht vom Eintritt eines Schadens abhängig sein. Solche Praktiken widersprechen per se schon der Menschenwürde und Persönlichkeitsrechten.
Auch bei **Techniken, die die Verletzlichkeit bestimmter Personengruppen ausnützen,** darf nicht die Eintrittswahrscheinlichkeit von Schäden eine Voraussetzung für ein Verbot sein, wie es der Entwurf vorsieht.

Ebenso sind die Einschränkungen beim **„social scoring"** kritisch zu hinterfragen. Auch wenn die behördliche Bewertung von sozialem Verhalten verboten wird, so bleiben trotzdem viele Spielarten von (grundrechtswidrigem) social scorings erlaubt. Ein Verbot von behördlichen social scoring soll nämlich nur für Daten gelten, die ursprünglich für andere Zwecke gesammelt wurden oder wenn die Benachteiligungen von Menschen, die dadurch entstehen, unverhältnismäßig zum sozialen (Fehl-) Verhalten sind. Werden hingegen Daten von vornherein zum Zweck des Scorings erhoben, so bleibt die Bewertung von sozialem Verhalten erlaubt. Das berührt aber rasch die Menschenwürde. 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 extrem lückenhaften Verbot nicht erfasst und dennoch grundrechtswidrig ist. Können Praktiken, die nach Art 5 nicht untersagt sind, mit Blick auf die EMRK oder Art 22 DSGVO verboten werden (etwa soziales Scoring durch die Privatwirtschaft oder Bewertungen von anderen Eigenschaften als der „Vertrauenswürdigkeit" einer Person)? Der Entwurf böte jedenfalls die Chance, auch Unzulänglichkeiten im Artikel 22 DSGVO zu beseitigen (Erweiterung des Schutzes auf statistische Gruppen, bei denen kein Personenbezug vorliegt 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 (Suche nach Verbrechensopfern, Lebensbedrohung von Personen, Terrorismus, Personensuche wegen schwerer Verbrechen). Begrüßt wird, dass der Einsatz solcher biometrischen 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, denn auch die biometrische Auswertung von Videomaterial kann tief in Grundrechte eingreifen. Arbeitspapiere der EU-Kommission enthielten noch ein mehrjähriges Verbot der KI-Analyse von biometrischen Merkmale für private wie öffentliche Akteure. Für den Grundrechtsschutz in der EU ist es das falsche Signal, wenn der Entwurf kein (zumindest temporäres) Einsatzverbot ausspricht. Neben Datenschutzbedenken besteht auch die Gefahr von falschen Ergebnissen aufgrund der Fehlerraten. Menschen geraten dabei irrtümlich ins Visier, obwohl sie nichts verbrochen haben.

Wichtige Regulierungsanliegen wären dabei:

- **Biometrie darf kein Geschäft werden**: Der Handel mit biometrischen Daten sollte verboten und mit hohen Strafen sanktioniert sein.
- **Wahlfreiheit ist oberstes Gebot**: Jede/r sollte selbst entscheiden können, ob seine/ihre biometrischen Daten verarbeitet werden dürfen oder nicht.

- **Pflichtcheck vor dem Griff nach biometrischen Daten**: Vor jedem Einsatz biometrischer Daten sollten Datenschutzbehörden angesichts des hohen Risiko- und Schadenspotenzials prüfen, ob die Verarbeitung biometrischer Daten notwendig und sinnvoll ist.
- **Onlinebanking und andere Anwendungen ohne bleibende biometrische Daten**: Es darf zu keiner dauerhaften Speicherung von biometrischen Daten kommen, um das Risiko von Identitätsdiebstahl zu minimieren.
- **Gesichtsfotos als sensible Daten**: Onlinefotos werden bereits in unzähligen Fällen für die Identifikation von Personen durch Gesichtserkennung genutzt.
  Rechtlich ist offen, inwieweit diese Daten als biometrisch gelten. Hier besteht dringend Bedarf, Porträts vor versteckter biometrischer Auswertung zu schützen.

Klassifizierung von KI-Systemen als hoch-riskant (Art 6)

Hochriskant sind KI-Systeme nur dann, wenn sie als Sicherheitskomponente oder -produkt nach den in Anhang II angeführten Harmonisierungsrechtsvorschriften gelten. Zusätzlich muss die Sicherheitskomponente bzw das Sicherheitsprodukt einer Konformitätsbewertung durch Dritte wiederum nach den in Anhang II angeführten Harmonisierungsrechtsvorschriften unterzogen werden.
KI wäre nur dann hochriskant, wenn sie mit einer externen Zertifizierung nach den „New Approach" RL über die technische Produktkonformität verbunden ist. Für die Qualifizierung eines KI-Sicherheitsproduktes als hochriskant kann aber nicht ernsthaft ausschlaggebend sein, ob es einer New Approach RL unterliegt und nach dieser extern zu zertifizieren ist (was im Übrigen selten der Fall ist). Dieser Ansatz ist verfehlt und 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, Betrugs- und Missbrauchserkennung aufgrund des Kundenverhaltens, werblich-manipulative Beeinflussung des Nutzerverhaltens, Produktempfehlungen, Nachrichtenselektion uvm).
Die EU-Kommission kann zwar den Annex III ergänzen, allerdings nur die bereits angelegten Kategorien um weitere Beispiele erweitern. Neue Kategorien sind ausgeschlossen. Damit können wichtige, verbraucherrelevante 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.

Anmerkungen zum Annex:

- Die Erfassung von „**KI-Systemen, die für die biometrische Echtzeit-Fernidentifizierung"** verwendet werden sollen ist zu eng. Biometrische KI-Systeme sind auch dort im Vormarsch, bei denen keine „Fern"-Identifikation stattfindet (Onlinebanking, Geräteentsperrung etc). Aufgrund der hohen Missbrauchsgefahr und den Fehlerraten sollten auch diese Anwendungen mitreguliert werden.
- Bei der „**Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen**" bedarf es erläuternder Beispiele, was darunterfällt.
- Die „**Kleinanbieter-Ausnahme für den Eigengebrauch**" in Bezug auf „KI-Systeme, die für die **Kreditwürdigkeitsprüfung und Kreditpunktebewertung"** verwendet werden sollen sollte kritisch hinterfragt werden. Risiken bestehen unabhängig von der Unternehmensgröße.
- „**KI-Systeme, die von Strafverfolgungsbehörden für individuelle Risikobewertungen** natürlicher Personen verwendet werden sollen, um das Risiko abzuschätzen, dass eine natürliche Person Straftaten begeht oder erneut begeht…" sollten zu den absolut verbotenen Praktiken zählen. Verletzung der Menschenwürde, hohe Fehlerraten, diskriminierende Bias uvm sind nur einige der Gründe, warum für derartige Anwendungen grundsätzlich kein Platz sein sollte.

Auch „KI-Systeme, die von Strafverfolgungsbehörden **als Lügendetektoren** und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustands einer natürlichen Person verwendet werden sollen“ sollten der Liste verbotener Praktiken hinzugefügt werden. Nicht nur als hochriskant, sondern in einer Demokratie als unannehmbar sollten außerdem KI-Systeme gelten, “die von Strafverfolgungsbehörden **zur Vorhersage des Auftretens einer tatsächlichen oder potenziellen Straftat auf der Grundlage des Profils natürlicher Personen** oder zur Bewertung von Persönlichkeitsmerkmalen und Eigenschaften oder vergangenen kriminellen Verhaltens natürlicher Personen oder von Gruppen verwendet werden sollen.“ Außerdem sind KI-Systeme, „die zur Kriminalanalyse natürlicher Personen eingesetzt werden sollen und es den Strafverfolgungsbehörden ermöglichen, große **komplexe verknüpfte und unverknüpfte Datensätze aus verschiedenen Datenquellen** oder in verschiedenen Datenformaten zu durchsuchen, **um unbekannte Muster zu erkennen oder verdeckte Beziehungen in den Daten aufzudecken**“ mit den Grundregeln des Datenschutzes unvereinbar und deshalb verboten.

Transparenz und Bereitstellung von Informationen für Nutzer (Art 13)
Es ist unakzeptabel, dass nur dem professionellen Anwender Informationen zum KI-Betrieb zugänglich sein müssen. Auch Betroffene haben einen Anspruch auf Transparenz. Die in Abs 3 genannten Informationen (Kontaktdaten, Merkmale des KI-Systems, Risiken für Gesundheit und Sicherheit etc.) 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. Unklar ist auch, 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 jedoch, dass sich diese Verpflichtungen sich nach der Größe des Unternehmens richten. Risiken müssen unabhängig von der Unternehmensgröße mit größter Sorgfalt 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 sehr 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 keine hinreichende Schutzmaßnahme. Ihr Einsatz sollte grundsätzlich zu den verbotenen Praktiken des Artikel 5 zählen.

Weiterverarbeitung personenbezogener Daten in KI- „Sandboxes/Reallaboren“ (Art 54)
In sogenannten KI-Reallaboren sollen personenbezogene Daten, die eigentlich für andere Zwecke erhoben wurden, zum Testen von KI benutzt werden dürfen, wenn ein erhebliches öffentliches Interesse besteht und mit anonymen Daten nicht das Auslangen gefunden werden kann. 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 und läuft auch Gefahr, einer EUGH-Kontrolle nicht stand zu halten.

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, als Proband zur Verfügung zu stehen. Die Datenschutzbehörde hat ein solches Vorhaben außerdem vorab zu prüfen und geeignete Auflagen zu erteilen oder zu untersagen.

Weitere Verbraucheranliegen:

Hersteller und Nutzer hochriskanter Anwendungen benötigen eine Haftpflichtversicherung:
Hersteller und Nutzer sollten gegenüber Betroffenen für materielle und immaterielle Schäden solidarisch haften müssen. Ebenso sollte eine diesbezügliche Versicherungspflicht bestehen.

leichte Rechtsdurchsetzung:
Es sind für Betroffene nationale Anlaufstellen einzurichten (für Beschwerden, Nachprüfungen von KI Ergebnissen, sowie bei grenzüberschreitenden Problematiken). Ebenso ist eine Verbandsklagsbefugnis und Beschwerdemöglichkeiten von Vertretungen zur Wahrung kollektiver Interessen von Betroffenengruppen vorzusehen.

Schutz vor Intransparenz, Diskriminierung und Manipulation in niedrigeren Risikoklassen:
Auch in niedrigeren Risikoklassen braucht es verbindliche Ge- und Verbote, die Transparenz, Diskriminierungsfreiheit und die Beachtung der Grundrechte sicherstellen. Eine Aufsichtsbehörde sollte Einblick in die technischen Prozesse erhalten und durch ein Zulassungsverfahren garantieren, dass keine diskriminierenden, die Informationsfreiheit und Meinungsvielfalt beeinträchtigende bzw datenschutzwidrige Entscheidungskriterien verwendet und darauf basierende Entscheidungen getroffen werden.

Schließen von Schlupflöchern in der DSGVO für den Einsatz intransparenter Algorithmen:
Derzeit sind nach DSGVO nur vollautomatisierte Einzelentscheidungen, die Rechtsfolgen haben oder KonsumentInnen erheblich beeinträchtigen, grundsätzlich verboten. Dieser Schutz sollte auf „halbautomatisierte“ Entscheidungen ausgedehnt werden, bei denen zwar Menschen entscheiden, aber Maschinen diese Entscheidung „vorbereiten“, denn Bewertungen werden von Mitarbeitern nachträglich selten abgeändert. Außerdem sollten Betroffene über jeden Algorithmus, der mit Daten von KonsumentInnen arbeitet, informiert werden - unabhängig von den Rechtsfolgen oder einer starken Beeinträchtigung der KonsumentInnen, wie es die DSGVO derzeit verlangt.
Die Erlaubnistatbestände des Artikel 22 gehen ebenfalls viel zu weit. Algorithmische Entscheidungen sind unter bestimmten Bedingungen zulässig (zB bei Abschluss bzw Erfüllung von Verträgen sofern KonsumentInnen die Möglichkeit haben die Entscheidung anzufechten). Der Einsatz bei Verbraucherverträgen sollte aber nur in besonders begründeten Fällen (wie einem hohen Zahlungsausfallsrisiko bei Krediten) möglich sein.

Ruf nach mehr Trainingsdaten für KI erfordert wirksameren Datenschutz:
Selbstlernende Systeme werden mit Trainingsdaten gefüttert um in riesigen Datenbeständen nach unerkannten Mustern und Zusammenhängen zu suchen. Werden personenbezogenen Daten genutzt, lässt das mit der Pflicht zur Datensparsamkeit, engen Zweckbindung und „privacy by design and default“ schwer in Einklang bringen. Ein Nachweis, wie dies im Einzelfall gelingt, ist von den Herstellern und Nutzern von KI unbedingt zu verlangen.

KI lässt sich mit zentralen Datenschutzprinzipien schwer vereinbaren. Dieser immanente Konflikt ist offen anzusprechen:
Der Entwicklung zu einer Datenökonomie stehen der Grundsatz der Datensparsamkeit und die Gebote von privacy by design bzw default entgegen. Viele ExpertInnen gehen zB davon aus, dass konkrete Personen auch aus anonymisierten Datensätzen durch Einsatz von KI individuell bestimmbar sind.

Es ist deshalb zu definieren, wann man noch von Daten ohne Personenbezug reden kann. (siehe dazu auch https://www.akeuropa.eu/de/evaluation-der-datenschutz-grundverordnung-dsgvo)
Die DSGVO enthält allgemeine Grundsätze, die die vielen Rechtskonflikte zwischen Geheimhaltungs- und Verwertungsinteressen nicht unmittelbar lösen können. Unzulässige Verarbeitungspraktiken auszuforschen und rechtlich richtig zu würdigen, überfordert nicht nur KonsumentInnen, sondern aufwandsbedingt zunehmend auch die Aufsichtsbehörden. Dies schadet der Rechtssicherheit und mindert das Vertrauen in die Vorteile von KI. Die Ausstattung der Behörden entspricht nicht dem Bedarf, um rasch, sorgfältig, technikkundig und investigativ den vielfältigen Aufsichtsaufgaben nachzukommen. Die Verlagerung von einer ex-ante Prüfpflicht in sensiblen Fällen zu einer nachträglichen Aufarbeitung von Rechtsverletzungen samt Schadenersatzansprüchen eröffnet schwerwiegende Schutzlücken, wenn Rechtsdurchsetzung nicht rasch und reibungslos funktioniert.

Verbot von Anwendungen, bei denen die „Accountability" an Grenzen stößt:
Mit der Selbstlernfähigkeit der Systeme können Softwareentwickler oft selbst nicht mehr nachvollziehen, welchen logischen Weg Algorithmen einschlagen. Entscheidet KI aber selbst darüber, welche Daten sie für welchen Zweck nutzt, widerspricht dies fundamental dem Rechtsgrundsatz der „Accountability" (Zurechnung, Verantwortung, Haftung), und kollidiert auch mit der Pflicht, im Erhebungszeitpunkt bereits den genauen Verwendungszweck der Daten anzugeben
Alle Entscheidungen, Produkte und Dienste die auf Algorithmen basieren, müssen erklär- und überprüfbar bleiben. KonsumentInnen dürfen angesichts einer Vielzahl an Beteiligten (Entwickler, Hersteller, Anwender, Dienstleister) nicht zum Spielball unklarer Verantwortlichkeiten werden. Sie sollen im Sinne einer Solidarhaftung Unterlassungs- und Schadenersatzansprüche gegen jeden Beteiligten in der Wertschöpfungskette richten können (mit anbieterseitigen Regressmöglichkeiten).

Einbindung der Betroffenen:
Daten- und Privatsphärenschutz sollten wirtschaftlichen Interessen grundsätzlich vorgehen. Wie verhält es sich aber, wenn Eingriffe in diese Rechte mit lebenswichtigen Interessen einzelner Personen, von Gruppen oder der Gesamtgesellschaft begründet werden? Interessenskollisionen sind vorprogrammiert, sobald KI-Anwendungen im Gesundheitssektor Verbesserung bei der Erkennung, Behandlung und Heilung von Krankheiten oder im sicherheitspolizeilichen Einsatz eine bessere Kriminalitätsprävention bzw -aufklärung versprechen. Der Preis für diesen (potentiellen) Fortschritt ist hoch: Interessen von großen Bevölkerungsteilen können damit gefährdet werden. Vor diesem Hintergrund braucht es für die Mehrzahl an KI-Anwendungen, die Grundrechte berühren, eine ex ante-Genehmigung durch ein unabhängiges Gremium. In dieses sind neben Datenschutzbehörden und Technikexperten auch VertreterInnen der jeweils betroffenen Gruppen (ArbeitnehmerInnen, KonsumentInnen, PatientInnen, etc) miteinzubeziehen. Denn auch bei der Klärung von Rechtsfragen wird sorgfältig zwischen verschiedenen Interessen, Verhältnismäßigkeiten, Werten etc. abzuwägen sein. Diese Entscheidungen können abhängig von der jeweiligen Betroffenheit und dem jeweiligen weltanschaulichen Hintergrund sehr verschieden ausfallen. Die gesellschaftliche Akzeptanz von Entscheidungen für oder gegen einzelne KI-Anwendungen und flankierende Auflagen fällt höher aus, wenn bei der Zusammensetzung des Entscheidungsgremiums auf eine breite Beteiligung aller betroffenen Gruppen geachtet wird.

Produkthaftungsregeln aktualisieren:
Die Produkthaftungs-RL aus dem Jahr 1985 kennt für digitale Trends wie KI keine Antworten. Eine überarbeitete RL muss auf alle materiellen und nicht materiellen Sachen, digitale Dienstleistungen und digitalen Inhalte anwendbar sein und sollte deshalb auch Cybersicherheitsrisiken, mangelnde Softwareupdates und unzureichende DSGVO-Konformität zu den „Defekten" eines Produktes zählen. Ebenso Schäden, die durch die Fähigkeit selbst zu lernen und autonome Entscheidungen zu treffen oder durch einen Missbrauch der verwendeten Daten entstehen. Ausgezeichnete Detailvorschläge für die Überarbeitung der Produkthaftungs-RL enthält das BEUC-Positionspapier „Product Liability 2.0"

Überholte Produktsicherheits-RL um KI-Risiken erweitern:
Die RL aus dem Jahr 2001 enthält zentrale Schutznormen, die Hersteller verpflichtet nur sichere Produkte in Verkehr zu bringen und VerbraucherInnen durch Informationspflichten und Warnhinweisen vor Risiken bewahrt. Es ist klarzustellen, dass auch die Produktsicherheits-RL auf alle Produkte, Dienste und Software, die Algorithmen/KI enthalten, anwendbar ist. Alle mit KI verbundenen Risiken müssen auch hier abgedeckt sein.

III. 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 propagiert. Es ist prinzipiell zu begrüßen, dass Künstlicher Intelligenz ein europäischer Rechtsrahmen gegeben werden soll. Doch der vorliegende Verordnungsentwurf enttäuscht auf vielen Ebenen und beschränkt sich auf eine sehr technikzentrierte Sicht auf den Binnenmarkt, während viele notwendige Rahmenbedingungen für ArbeitnehmerInnen und KonsumentInnen keine Erwähnung finden. Der „Menschenzentrierte Ansatz" bleibt hier zugunsten eines liberalen Marktes für KI oft auf der Strecke.
Europa sollte hier eine Führungsrolle übernehmen und alle Interessen zum gemeinsamen Nutzen zu berücksichtigen. Dazu bedarf es allerdings der Ergänzung und Präzisierung des geplanten Rechtsrahmens um hohe Sicherheitsstandards für alle zu ermöglichen und insbesondere auch einen hohen Grundrechtsschutz aufrecht zu erhalten.

Die wichtigsten Eckpunkte wären dabei:

- **Regeln nicht ausschließlich für Hochrisiko Anwendungen:**

Auch weniger risikobehaftete KI bedarf eines Regelwerks

- **Mitbestimmung**:
  Die Einbindung Betroffener ist essentiell. Nicht nur im Bereich der Grundrechte ist eine stärkere Einbindung von Betroffenen sinnvoll. Insbesondere beim Einsatz von KI im Arbeitsumfeld ist ein hohes Maß an betrieblicher und überbetrieblicher Mitbestimmung durch ArbeitnehmerInnen und ihrer Vertretungen notwendig. Sowohl im laufenden Betrieb als auch bei der Einführung solcher Anwendungen sollten MitarbeiterInnen bzw ihre Interessensvertretungen im Sinne eines Bottom-Up-Ansatzes stets umfangreich eingebunden sein. Das führt auch dazu, dass die Einführung von KI-Systemen in Produktions- und Organisationsabläufen wesentlich zielgerichteter und besser gestaltet werden kann, ArbeitnehmerInnen und ihre Vertretungen frühzeitig eingebunden werden und die Projekte von Anfang an begleiten und mitgestalten können. Deshalb sollte auch hier mehr Augenmerk daraufgelegt werden, dies aktiv zu fördern.
- **KI im Arbeitszusammenhang sollte prinzipiell als Hochrisiko-Anwendung gelten**
- **Rechte und Pflichten klar verankern**

Beschwerdemöglichkeiten bei unabhängigen Stellen, Informationspflichten nicht nur für professionelle Anwender, 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.

- **Nein zu einer umfassenden 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. Nicht einmal die Hersteller selbst können immer das (zukünftige) Verhalten von selbstlernenden Systemen vorhersagen. 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 und Einschränkungen stark durchlöchert. In der Praxis bleibt oft vom Bekenntnis zu einem umfassenden Schutz von Grundrechten, Datenschutz, ArbeitnehmerInnen-Schutz, dem Schutz der Privatsphäre und ähnlichem nicht mehr viel übrig. Grundsätzlich verbotene Praktiken wirken stark aufgeweicht, notwendige Teilbereiche werden nicht abgedeckt.

- **effektiver Rechtsschutz**

Rechtsschutzmöglichkeiten für einzelne aber auch durch kollektive Interessensvertretungen (zB im Wege von Verbandsklagen) müssen umfassend zugänglich sein. Auch auf eine ausreichende Ressourcenausstattung der Vollzugs- bzw Kontrollbehörden (inklusive Arbeitsinspektorate) ist dabei zu achten.

- **Aus- und Weiterbildung**

KI am Arbeitsplatz bedarf einer Verpflichtung zu vorbeugenden Maßnahmen wie Aus- und Weiterbildung. Das schützt ArbeitnehmerInnen und versetzt sie in die Lage, die Rolle von Daten und KI, sowie ihren Einfluss auf Arbeitsorganisation zu verstehen. Neue Technologien enthalten Unsicherheiten und unbekannte Risiken, darum müssen Prävention und das Vorsorgeprinzip Teil des regulatorischen Rahmenwerks sein.

- **Ungewünschte Anwendungen verbieten**

KI ermöglich durch den permanenten Strom an Daten bisher ungeahnte Möglichkeiten. (Beiläufig) anfallende Daten können mittels Algorithmen benutzt werden um Betroffene zu überwachen, zu kontrollieren, zu bewerten und sie zu identifizieren (auch nachträglich aus anonymisierten Daten). Sowohl im Arbeitszusammenhang, als auch bei KonsumentInnen bedarf es deshalb strenger Regelungen und Mitbestimmungsmöglichkeiten. **Bestimmte Anwendungen sollten dabei gänzlich verboten sein.**

- **ArbeitnehmerInnenschutz und Inklusion**

Der Sicherheit und Gesundheit am Arbeitsplatz sollte ein wichtiger Stellenwert eingeräumt werden. Schutz vor körperlichen und psychischen Risiken ist für ArbeitnehmerInnen wichtig. Gerade im Hinblick auf Arbeitsunfälle und arbeitsbedingten Erkrankungen bedarf es ausreichender Kontrollmöglichkeiten und der unabhängigen Zertifizierung von Systemen. Wie bei der CE-Kennzeichnung zu sehen ist, führt eine Selbstkontrolle zu lückenhafter Sicherheit, deren Mängel zu Arbeitsunfällen und Berufskrankheiten führen können. Deren Folgen werden externalisiert und die Kosten den Sozialversicherungen sowie zum Großteil den betroffenen ArbeitnehmerInnen selber aufgebürdet. Unternehmen haben zudem ein Interesse daran, ein „Minimum Viable Product“ auf den Markt zu bringen, um Entwicklungskosten gering zu halten. Demgegenüber braucht ArbeitnehmerInnenschutz aber höchstmöglich sichere Maschinen oder Technologien. In diesem Spannungsfeld ist die EU gefragt, die ArbeitnehmerInnen zu schützen. Ebenso fehlt auch eine stärkere Berücksichtigung von Menschen mit Behinderungen (zB Hör- und Sehdefizite) in der Betrachtung.

- **Entwicklungs- und Anpassungsmöglichkeiten der VO schaffen**

Die Taxonomie der Anwendungen im Anhang wird sehr starr definiert. Erweiterungen dürfen nur innerhalb existierender Kategorien erfolgen, neue Felder dürfen hingegen nicht aufgenommen werden. Angesichts der Dynamik des technischen Fortschritts sich stetig verändernder Anwendungsfelder für KI, sollte hier mehr Raum für Adaptierungen gelassen werden um auch auf zukünftige Probleme und Herausforderungen reagieren zu können.

Für Informationen stellen wir Ihnen jederzeit zur Verfügung:

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