AK EUROPA

Positionspapier
Februar 2026
Digital

Digitaler Omnibus

COM(2025) 836
COM(2025) 837

Zusammenfassung

Das vorgeschlagene Omnibus-Paket VII (COM(2025) 836 und 837 final) ist weit mehr als von der Kommission vorgeschobene bloße Vereinfachung bestehender Regelungen. Vielmehr werden mit diesem Paket gravierende Änderungen vorgeschlagen, womit ein Herabsenken des derzeitigen Verbraucher- und Datenschutzniveaus droht.

Kritik an Vorgangsweise durch Omnibus-Gesetzgebung

Die Kommission schlägt mittels eines beschleunigten Gesetzgebungsverfahrens, das für Änderungen rein technischer Natur vorgesehen ist, weitreichende Änderungen vor. Dies widerspricht den von der Kommission einzuhaltenden Grundsätzen der Verhältnismäßigkeit und der Subsidiarität. Ohne umfassende Folgenabschätzung und ausreichendes Daten- und Zahlenmaterial, das die Notwendigkeit der vorgeschlagenen Regelungen untermauern kann, steht die Möglichkeit einer Annullierung dieser beiden Rechtsakte im Raum.

Die AK hat die von der Kommission vorgeschlagenen Änderungen in der Datenschutz-Grundverordnung (DSGVO) und in der Verordnung über künstliche Intelligenz (KI-VO) eingehend analysiert.

Folgende Verschlechterungen sind dabei zu befürchten:

In der DSGVO:

- **Einschränkung des Anwendungsbereichs**
  Die Kommission schränkt die Einordnung pseudonymisierter Daten als personenbezogene Daten erheblich ein und schafft mit der eingeräumten Kompetenz zu Durchführungsrechtsakten weitere Möglichkeiten, den Anwendungsbereich näher zu definieren und dadurch einzuschränken.

- **Ausdehnung des „Forschungsprivilegs“ durch weite Definition von „wissenschaftlicher Forschung“**
  Wissenschaftliche Forschung wird nach dem Vorschlag der Kommission zu weit definiert; selbst überwiegend kommerzielle Zwecke verhindern nicht die Einordnung als wissenschaftliche Forschung. Damit werden die für die wissenschaftliche Forschung bereits bestehenden Privilegien ungebührlich ausgedehnt.

- **Privilegierung der Verarbeitung ‚sensibler Daten‘ für KI-Training und KI-Betrieb**
  Besondere Kategorien personenbezogener Daten sollen für Zwecke des KI-Trainings und des KI-Betriebs zulässig sein. Für eine derartige Privilegierung besteht keine Notwendigkeit; die derzeit geltenden Bestimmungen der DSGVO sind auch für KI-Betreiber ausreichend.

- **Einschränkung der Ausübung des Auskunftsrechts**
  Das Auskunftsrecht als das zentrale Betroffenenrecht soll nach dem Vorschlag der Kommission dahingehend eingeschränkt werden, dass dieses nur noch für Zwecke des Datenschutzes beantragt werden darf.

- **Einschränkung der Informationspflichten von Verantwortlichen**
  Bereits nach geltendem Recht können die Informationspflichten eingeschränkt werden, wenn der Betroffene bereits über die Informationen verfügt. Nunmehr sollen diese Informationspflichten noch weiter eingeschränkt werden. Es droht die Erschwerung der Ausübung der Betroffenenrechte mangels ausreichender Informationen.

- **Erleichterung der automatisierten Einzelfallentscheidungen mit Auswirkungen für Betroffene**
  Derzeit besteht ein generelles Verbot von ausschließlich automatisierten Entscheidungen; eine

automatisierte Entscheidung ist nur in gesetzlich aufgelisteten Fällen wie zB vertragliche Notwendigkeit oder ausdrückliche Einwilligung des Betroffenen zulässig. Die Kommission möchte von diesem generellen Verbot abkehren und eine automatisierte Entscheidung leichter ermöglichen.

- **Unklarheiten durch Aufteilung der bisherigen „cookie"-Bestimmung in DSGVO und e-privacy-Richtlinie**
  Die Verarbeitung von nicht-personenbezogenen Daten im Zusammenhang mit Endeinrichtungen soll in der e-privacy-Richtlinie bleiben, jene von personenbezogenen Daten in Endeinrichtungen soll in die DSGVO wandern, wobei auch neue Rechtmäßigkeitsgründe für die Verarbeitung von personenbezogenen Daten in Endeinrichtungen vorgeschlagen werden. Dies führt zu erheblichen Unklarheiten in der Rechtsanwendung.

In der KI-VO:

- **Erweiterung von Ausnahmen auf sogenannte ‚Small Mid-Cap' Unternehmen (SMC)**
  Die KI-VO als Produktsicherheitsrecht knüpft primär am Risiko des KI-Systems an und nicht an der Größe des Unternehmens. Die bereits für kleine und mittlere Unternehmen in der KI-VO bestehenden Vereinfachungen sollten daher nicht auf sogenannte Small Mid-Cap Unternehmen ausgedehnt werden. Damit drohen wichtige Qualitätssicherungsmaßnahmen nach der KI-VO für Hochrisiko-KI-Systeme nicht angewandt zu werden.

- **KI-Kompetenz als bloße Empfehlung**
  KI-Kompetenz des Personals und anderer Personen, die mit KI-Systemen befasst sind, muss sichergestellt sein, andernfalls fehlt es Bediener:innen an Kompetenz im Umgang mit KI-Systemen und die nach der KI-VO nötige menschliche Aufsicht wird erheblich erschwert.

- **Ausweitung der Zulässigkeit der Verarbeitung sensibler Daten für sämtliche KI-Systeme**
  Besondere Kategorien personenbezogener Daten (‚sensible Daten') sollen nunmehr nicht nur im Bereich von Hochrisiko-KI-Systemen, sondern generell für Anbieter und Betreiber sämtlicher KI-Systeme zum Zweck der Erkennung und Korrektur von Verzerrungen verarbeitet werden. Dies stellt eine unzulässige Ausweitung und Privilegierung zulasten des Grundrechts auf Schutz personenbezogener Daten dar.

- **Entfall der Registrierungsverpflichtung**
  KI-Systeme, die aus Unternehmersicht keine Hochrisiko-KI-Systeme darstellen, sollen nach dem Vorschlag der EK nun nicht mehr registriert werden. Damit entfällt jegliche Schutzmaßnahme für Transparenz, öffentliche Rechenschaftspflicht und Aufsicht.

- **Verzögerung des Geltungsbeginns**
  Die EK schlägt ein Hinausschieben des Geltungsbeginns vor, womit weitere Rechtsunsicherheit droht.

Die Position der AK

Mit dem vorgelegten digitalen Omnibus-Paket VII (COM(2025) 836 final sowie COM(2025) 837 final) beabsichtigt die Europäische Kommission unter dem Schlagwort „Vereinfachung" („simplification") teilweise umfassende Änderungen einer Reihe von Rechtsakten. Via Omnibus-Rechtsakt sollen nicht nur mitunter erst seit kurzer Zeit bzw. noch gar nicht vollständig in Geltung stehende Rechtsakte wie die Datenverordnung oder die Verordnung über künstliche Intelligenz (KI-VO) wieder geändert werden, sondern es werden ohne Not auch umfassende Änderungen von wichtigen Schutzregelungen in der Datenschutz-Grundverordnung (DSGVO) vorgeschlagen.

Aus Sicht der AK ist die Weiterentwicklung der Innovationskraft und Wettbewerbsfähigkeit der europäischen Digitalindustrie wichtig, um Arbeitsplätze, Wertschöpfung und digitale Souveränität in Europa zu stärken. Dabei muss allerdings der Mensch im Mittelpunkt der Regelungen stehen. Die Aufrechterhaltung eines hohen Datenschutzniveaus und der Schutz der Privatsphäre sowie eine KI-Regulierung, die klare Regeln, Rechtssicherheit und den Schutz der Nutzer:innen und Betroffenen im Fokus hat, sind dabei essenziell. Es darf keinesfalls zu Rückschritten beim bestehenden Schutzniveau kommen.

Kritik an Vorgangsweise durch Omnibus-Gesetzgebung

Die Europäische Kommission legt mit dem digitalen Omnibus-Paket unter dem Schlagwort Vereinfachung (engl. „simplification") nicht nur gezielte und technische Änderungen in verschiedenen Rechtsakten vor, sondern schlägt de facto umfassende, gravierende und teilweise die Grundrechte (u.a. Art 8 Schutz personenbezogener Daten und Art 38 Verbraucherschutz der Grundrechtecharta [GRCh]) einschränkende Regelungen vor. Unter dem Deckmantel vermeintlicher „Vereinfachungen" auf lediglich technischer Ebene werden mit den Omnibus-Paketen in demokratiepolitisch höchst fragwürdiger Weise Schwächungen und Verwässerungen bestehender gemeinwohlorientierter Standards verfolgt.

Den einleitenden Ausführungen der Kommission zu den beiden Rechtsakten COM(2025) 836 und 837 final, dass die Änderungen bloß technischer Natur sind, eine Folgenabschätzung demnach nicht erforderlich ist und das vorliegende ‚Staff Working Document' (SWD(2025) 836 final) als Grundlage ausreicht, kann daher keinesfalls gefolgt werden.

Die Kommission verwendet das Vehikel der Omnibus-Gesetzgebung, das ursprünglich für rein technische und geringfügige Änderungen vorgesehen war, für umfassende Änderungen mit weitreichenden Folgen. Sie bedient sich eines Eilverfahrens, ohne die im ordentlichen Gesetzgebungsverfahren notwendigen Schritte einzuhalten. Im Sinne der stets einzuhaltenden Grundsätze der Verhältnismäßigkeit und der Subsidiarität, also der Prüfung, ob der vorgeschlagene Rechtsakt das analysierte und mit Zahlen und Fakten belegte Problem der einzige Weg und verhältnismäßig zur Erreichung des erklärten Ziels ist, bedarf es einer umfassenden öffentlichen Konsultation, einer Folgenabschätzung mit zusätzlicher eingehenderer Prüfung, da Grundrechte beeinträchtigt werden sowie einer Analyse von Alternativen.

Gemäß Art 2 des Protokolls (Nr. 2) zum Vertrag über die Arbeitsweise der Europäischen Union über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit hat die Kommission umfangreiche Konsultationen durchzuführen, bevor sie einen Gesetzgebungsakt vorschlägt. Bei dem hier vorgelegten digitalen Omnibus-Paket waren die vorgeschlagenen Änderungen in der DSGVO sowie in der KI-Verordnung nicht Teil einer vorangegangenen Konsultation. Erst nach Vorlage der Gesetzesvorschläge hat die Kommission nunmehr eine Konsultation hierzu bzw. zum bloß die KI-VO betreffenden Teil gestartet. Diese Vorgangsweise ist keinesfalls im Einklang mit den Prinzipien der Subsidiarität und der Verhältnismäßigkeit. Auch die „Better Regulation Toolbox", zu deren Einhaltung sich die Kommission zwecks besserer Rechtssetzung verpflichtet hat, schreibt vor, dass für einen Rechtsakt mit derart weitreichenden Änderungsvorschlägen (wie zB Einschränkung des Anwendungsbereichs der DSGVO) für die Wahrung der Prinzipien der Subsidiarität und der Verhältnismäßigkeit eine umfassende Folgenab-

schätzung sowie weitreichende Konsultationen und Stakeholder-Konsultationen durchzuführen sind. Damit sollen umfassende Informationen und Nachweise gesammelt werden, die die Notwendigkeit dieses beabsichtigten Rechtsaktes darlegen und untermauern.

In Bezug auf das Omnibus-I-Paket hat die Europäische Ombudsstelle mehrere Verfahrensmängel festgestellt, darunter die mangelnde Berücksichtigung der „Better Regulation Guidelines" durch die Europäische Kommission. Auch die Vorgehensweise der Erarbeitung des „Digital Omnibus"-Pakets zeichnet sich unserer Ansicht nach durch fehlende Beachtung von Prinzipien der „good governance" aus – die zu einer unausgewogenen Sichtweise hinsichtlich der möglichen Auswirkungen der Vorschläge beitragen.

Die Kommission verstößt mit ihrer Vorgehensweise daher gegen verfassungsrechtliche Grundprinzipien, die sie nochmals in der interinstitutionellen Vereinbarung zwischen Parlament, Rat und Kommission bekräftigt hat. Die Unzulässigkeit dieser Vorgangsweise kann schließlich durch EuGH-Judikatur untermauert werden. Diese Rechtsakte bergen sohin die Gefahr einer Annullierung, weshalb die gravierenden Änderungsvorschläge in diesen Rechtsakten bereits aus diesem Grund entschieden abzulehnen sind.

- **Artikel 1 – Data Act:**

Die Zusammenführung der verschiedenen Rechtsakte zur Datenverfügbarkeit und Datenwirtschaft (DA, DGA, ODD, FFDR) wird grundsätzlich begrüßt.
Abgelehnt wird allerdings die Verwässerung der Unabhängigkeit der Datenvermittlungs-Dienste, da deren strukturelle Unabhängigkeit zur Änderung der Grundlagen der Datenwirtschaft beitragen soll, indem Daten neutral und ohne Eigeninteressen eines Unternehmens verwaltet und zur Verfügung gestellt werden.
Abgelehnt wird weiters aus demselben Grund die Schwächung der Berichtspflicht der Daten-Altruismus-Organisationen: Nur wenn diese absolut vertrauenswürdig sind und der regulatorischen Aufsicht unterliegen, kann gewährleistet sein, dass personenbezogene Daten im Bereich bspw. der medizinischen Forschung zur Verfügung gestellt werden können.

Datenschutz-Grundverordnung (DSGVO)

- **Art 4 Z 1 und Art 41a DSGVO – Definition „personenbezogene Daten" und Pseudonymisierung**

Nach geltendem Recht fallen pseudonymisierte Daten in den Anwendungsbereich der DSGVO, wenn der Personenbezug wiederhergestellt werden kann. Dies gilt, auch wenn nur ein Dritter über die erforderliche Zuordnungsregel verfügt und diese Zuordnung vornehmen kann (siehe dazu EuGH Rs C-582/14 – Breyer). Für eine Einstufung als personenbezogene Daten im Sinne des Art 4 Abs 1 DSGVO ist es demnach nicht erforderlich, dass „sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden". Zudem soll der Begriff laut EuGH weit verstanden werden (siehe EuGH Rs. C-413/23 P – EDSB g SRB, Rn 54 und 99). Der EuGH führt hierin nämlich u.a. aus, dass Pseudonymisierung – je nach den Umständen des Falles – andere Personen als den Verantwortlichen tatsächlich daran hindern kann, die betroffene Person zu identifizieren, so dass diese für sie nicht oder nicht mehr identifizierbar ist. Allerdings können an sich nicht personenbezogene Daten dann zu „personenbezogenen" Daten werden, wenn der Verantwortliche sie anderen Personen überlässt, die über Mittel verfügen, die nach allgemeinem Ermessen wahrscheinlich die Identifizierung der betroffenen Person ermöglichen.

In **Art 4 Z 1 DSGVO** soll nun ein Zusatz bei der Definition von „personenbezogenen Daten" angefügt werden, wonach Daten nicht mehr als personenbezogen einzuordnen sind, wenn der Personenbezug nicht mit den vernünftigerweise verwendeten Methoden hergestellt werden kann, weil zB nur ein Dritter die erforderliche Zuordnungsregel kennt.

Die verkürzte Wiedergabe der Rechtsprechung führt unweigerlich zu Auslegungsproblemen, und potenziell zu einer zu weiten und irreführenden Anwendung, die unverhältnismäßig in das Grundrecht auf Datenschutz eingreift. Die Einordnung pseudonymisierter Daten als personenbezogene Daten und somit der Anwendungsbereich der DSGVO wird durch diesen Zusatz erheblich eingeschränkt. Die Anwendung der DSGVO kann damit schnell umgangen werden; Verantwortliche können durch die Übermittlung pseudonymisierter Daten an Dritte die Daten zu Unrecht dem Schutz der DSGVO entziehen. Zudem bezieht sich die vorgeschlagene Formulierung nicht auf die Pseudonymisierung, sondern enthält sehr allgemein gehaltene Formulierungen.

Darüber hinaus können Betroffene schwer bis kaum beurteilen, ob es sich bei Daten für ein bestimmtes Unternehmen nun um personenbezogene handelt oder nicht, ob also zB ein Unternehmen die Mittel, die vernünftigerweise eingesetzt werden können, hat. Damit wird Betroffenen, aber auch jedem:jeder anderen Außenstehenden die Einordnung in den Anwendungsbereich der DSGVO erschwert bzw. nahezu unmöglich gemacht und die daraus resultierende mögliche Anwendbarkeit der Betroffenenrechte verschleiert.
Ein Beitrag zur „Vereinfachung" ist dies keineswegs.

Die derzeitige Definition personenbezogener Daten nach Art 4 Abs 1 DSGVO sollte daher aus Sicht der AK bestehen bleiben und keinesfalls eingeschränkt werden.

Damit in Zusammenhang steht auch der vorgeschlagene **Art 41a DSGVO**. Danach soll der Kommission die Kompetenz zu Durchführungsrechtsakten eingeräumt werden, um die Mittel und Kriterien zur Bestimmung, ob es sich aufgrund von Pseudonymisierung nicht mehr um personenbezogene Daten handelt, näher festzulegen. Eine derartige Möglichkeit, mittels Durchführungsrechtsakten über die Einordnung in den Anwendungsbereich der DSGVO entscheiden zu können, wird seitens der AK entschieden abgelehnt. Art 41a DSGVO sollte daher – ebenso wie der vorgeschlagene Zusatz in Art 4 Z 1 DSGVO – ersatzlos gestrichen werden.

Seitens der AK wird bezweifelt, dass eine derartige Regelung – aufgrund der eingangs erläuterten einzuhaltenden Grundsätze – einer Prüfung vor dem EuGH nach Art 263 AEUV standhalten wird.

- **Formale Anmerkung zu Art 4 DSGVO**

Die Kommission schlägt für Art 4 das Hinzufügen mehrerer Begriffsbestimmungen vor, die Nummerierung ist hier jedoch nicht fortlaufend. Selbst unter Berücksichtigung der von der EK vorgeschlagenen Begriffsbestimmungen im Omnibus IV-Paket (COM(2025) 501 final), womit die Ziffern 27 und 28 eingefügt werden sollen, gibt es für die Ziffern 29 bis 31 des Art 4 keine Vorschläge der EK für Begriffsbestimmungen. Die fortlaufende Nummerierung im vorliegenden digitalen Omnibus sollte daher für „terminal equipment" mit Ziffer 29 (anstelle von Ziffer 32) starten.

- **Art 4 Z 38 DSGVO „scientific research" und Informationspflichten nach Art 13 DSGVO**

In einem neuen Art 4 Z 38 DSGVO, der richtigerweise mit Ziffer 35 nummeriert werden sollte, wird eine Definition für „scientific research" („wissenschaftliche Forschung") eingefügt. Danach soll jede Forschung, die Innovation wie etwa technologische Entwicklungen unterstützt, als eine wissenschaftliche verstanden werden. Diese Definition ist sehr weit gefasst, mit dem letzten Satz wird sogar die Möglichkeit eingeräumt, mit der Forschung kommerzielle Interessen zu verfolgen. Damit fällt etwa auch „Forschung" von Großkonzernen, die überwiegend kommerzielle Zwecke verfolgen, unter diese Definition. Eine derartig weite Definition des Begriffs ‚wissenschaftliche Forschung' hat weitreichende Folgen, zumal diese Begriffsbestimmung in Zusammenschau mit dem neu eingefügten Absatz 5 in Art 13 DSGVO, aber auch mit den übrigen Bestimmungen der DSGVO, die sich auf wissenschaftliche Forschung beziehen, zu lesen und zu beurteilen ist.

Art 13 DSGVO regelt die Informationspflichten bei Erhebung von personenbezogenen Daten bei der betroffenen Person. Nach dieser Bestimmung müssen Betroffene – neben Eckdaten zu Verantwortlichen – zum Zeitpunkt der Datenerhebung auch über ihre Betroffenenrechte, zB über ihr Auskunfts- und Löschungsrecht informiert werden.

Nach dem neu vorgeschlagenen, anzufügenden Absatz 5 des Art 13 sollen diese Informationen im Zusammenhang mit der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung nicht erteilt werden, wenn dies unmöglich oder – unter Verweis auf Art 89 Abs 1 DSGVO – mit unverhältnismäßigem Aufwand verbunden ist.

Eine derart weite Definition in § 4 Z 38 DSGVO ist daher angesichts dieser weit reichenden, negativen Auswirkungenstrikt abzulehnen, da weniger Information für Betroffene bereitgestellt wird. Für eine Einschränkung der Informationspflichten besteht aus Sicht der AK keine Notwendigkeit, weshalb Art 13 Abs 5 des Vorschlags zur DSGVO ersatzlos zu streichen ist.

Darüber hinaus sollte jedenfalls vermieden werden, dass durch die Einfügung der weiten Definition auch die Auslegung der Art 5 Abs 1 lit b und e, Art 9 Abs 2 lit j, Art 14 Abs 5 lit b, Art 17 Abs 3 lit d, Art 21 Abs 6 und des Art 89 DSGVO geändert wird, zumal auch hier dieser Begriff verwendet wird.

Aus Sicht der AK sollte – wie eingangs bereits erwähnt – die bisherige Auslegung der DSGVO nicht in Frage gestellt oder gar zu Ungunsten der Betroffenen geändert werden. Die vorgeschlagenen Ergänzungen in Art 4 und Art 13 DSGVO sollten daher gestrichen werden.

- **Art 5 DSGVO – Grundsätze für die Verarbeitung personenbezogener Daten**

Art 5 DSGVO normiert Grundsätze für die Verarbeitung personenbezogener Daten. Neben dem Grundsatz der Datenminimierung und der Richtigkeit wird in Abs 1 lit b leg cit der Grundsatz der Zweckbindung normiert.

In Art 5 Abs 1 lit b des Vorschlags zur DSGVO wird die zweifache Verneinung im letzten Satz *„not to be considered incompatible"* aufgelöst und durch *„be considered compatible"* ersetzt. Diese Änderung ist aus Gründen der besseren Lesbarkeit zu begrüßen. Darüber hinaus wird nach dem Vorschlag jedoch im letzten Halbsatz angefügt, dass der Grundsatz der Zweckbindung ‚*unabhängig von den Bedingungen des Art 6 Abs 4 der DSGVO*' einzuhalten ist.

Art 6 Abs 4 DSGVO regelt die Möglichkeit der Verarbeitung von personenbezogenen Daten zu einem anderen Zweck unter bestimmten Voraussetzungen. Diese Bestimmung ist nach dem vorgeschlagenen Zusatz in Art 5 Abs 1 lit b DSGVO nun nicht mehr zu berücksichtigen. Die AK spricht sich gegen den vorgeschlagenen Zusatz in Art 5 Abs 1 lit b DSGVO aus; für eine Abkehr von Art 6 Abs 4 DSGVO im Zusammenhang mit dem Grundsatz

der Zweckbindung gibt es keine sachliche Rechtfertigung; dies geht weit über eine bloß technische Anpassung hinaus.

Abzulehnen ist hier auch, wie bereits bei Art 4 Z 38 des Vorschlags zur DSGVO angemerkt, die weite Definition des Begriffs „scientific research". Dieser Begriff wird auch in Art 5 Abs 1 lit b DSGVO verwendet, wonach die Weiterverarbeitung der personenbezogenen Daten ua für wissenschaftliche Forschungszwecke („scientific research purposes") als vereinbar mit den ursprünglichen Zwecken gilt. Mit einem derart weiten Verständnis des wissenschaftlichen Forschungszweckes wird das Prinzip der Zweckbindung zu Ungunsten der Betroffenen ausgehöhlt; diese Definition ist daher auch im Lichte des Art 5 Abs 1 lit b DSGVO abzulehnen.

- **Art 9 DSGVO – Verarbeitung besonderer Kategorien personenbezogener Daten**

In Art 9 Abs 1 DSGVO wird für besondere Kategorien personenbezogener Daten („sensible Daten"), zB für Daten, aus denen die ethnische Herkunft oder weltanschauliche Überzeugungen hervorgehen, biometrische Daten oder Gesundheitsdaten, ein Verarbeitungsverbot normiert.

In Art 9 Abs 2 DSGVO werden Erlaubnistatbestände normiert, die die Verarbeitung sensibler Daten erlauben, so zB bei ausdrücklicher Einwilligung des Betroffenen in die Datenverarbeitung.

Die Verarbeitung dieser besonderen Kategorien personenbezogener Daten soll nach **Art 9 Abs 2 lit k** des Vorschlags zur DSGVO nunmehr auch für die Entwicklung und den Betrieb („development and operation") eines KI-Systems oder eines KI-Modells unter den Prämissen des neuen Art 9 Abs 5 DSGVO zulässig sein.

Nach diesem **Art 9 Abs 5** des Vorschlags zur DSGVO sollen geeignete organisatorische und technische Maßnahmen implementiert werden, um die Erhebung und anderweitige Verarbeitung von sensiblen Daten zu verhindern. Sollten dennoch sensible Daten im Datensatz des KI-Systems zu finden sein („residuale sensible Daten"; siehe dazu Erwägungsgrund 33 des Vorschlags), so muss der Verantwortliche diese entfernen. Ist deren Löschung mit unverhältnismäßigem Aufwand verbunden, haben Verantwortliche die Daten zumindest davor zu schützen, dass mit ihnen Output generiert wird oder diese veröffentlicht oder anderweitig für Dritte zugänglich gemacht werden.

Art 9 Abs 2 lit k des Vorschlags zur DSGVO schreibt nun die Zulässigkeit der Verarbeitung dieser übrig gebliebenen (im Sinne des Art 9 Abs 5 DSGVO-Vorschlag nicht löschbaren) sensiblen Daten im Zusammenhang mit der Entwicklung und dem Betrieb eines KI-Systems oder eines KI-Modells vor. Ergänzend sind hier die Ausführungen in Erwägungsgrund 33 heranzuziehen, wonach die Verarbeitung dieser residualen sensiblen Daten für den Verarbeitungszweck nicht notwendig sein darf. Sollten diese sensiblen Daten hingegen notwendig sein, so müssen die anderen Ausnahmetatbestände des Art 9 Abs 2 geprüft werden.

Bei diesem Regelungsvorschlag handelt es sich aus Sicht der AK um einen nicht gerechtfertigten und viel zu weit gefassten Versuch einer Privilegierung zugunsten der Entwicklung und des Betriebs eines KI-Systems bzw. KI-Modells. Aus Sicht der AK sind die vorgeschlagenen Ergänzungen daher zu streichen. Es ist nicht einzusehen und nicht rechtfertigbar, dass KI-Systementwickler:innen und -betreiber:innen eine derartige Privilegierung bei der Verarbeitung von sensiblen Daten zugutekommt. Wie andere Verantwortliche können und sollten auch KI-Systementwickler:innen und -betreiber:innen die Grundsätze der DSGVO zur Wahrung der Grundrechte auf Achtung des Privat- und Familienlebens und auf den Schutz personenbezogener Daten (Art 7 und 8 der Charta der Grundrechte der EU) einhalten.

Bei der Verarbeitung von sensiblen Daten sollen daher die Ausnahmetatbestände nach Art 9 Abs 2 lit a bis j DSGVO geprüft werden, wobei die Ausnahmen des Abs 2 eng auszulegen sind (siehe EuGH Rs C-667/21 – Medizinischer Dienst der Krankenversicherung Nordrhein). Eine unter Art 9 Abs 2 DSGVO subsumierte Verarbeitung sensibler Daten hat dabei im Sinne des Erwägungsgrundes 51 zur DSGVO sowie im Lichte der Rechtsprechung des EuGH die allgemeinen Grundsätze hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung nach Art 6 DSGVO einzuhalten (siehe EuGH Rs C-667/21 – Medizinischer Dienst der Krankenversicherung Nordrhein).

Die Verarbeitung von sensiblen Daten nach Art 9 Abs 2 lit k des Entwurfs zur DSGVO muss daher auch eine der in Art 6 Abs 1 DSGVO genannten Rechtmäßigkeitsvoraussetzungen erfüllen. Hier kommt sodann Art 88c des Entwurfs zur DSGVO ins Spiel, wonach sich Verantwortliche im Zusammenhang mit Entwicklung und Betrieb eines KI-Systems oder KI-Modells auf ein berechtigtes Interesse im Sinne des Art 6 Abs1 lit f DSGVO stützen können, wobei auch noch auf zusätzliche in Art 88c des Entwurfs einzuhaltende Schutzmaßnahmen hingewiesen wird.

In diesem Zusammenhang ist auch Art 4a des Entwurfs zur KI-VO zu erwähnen, der nach dem Vorschlag der EK nunmehr sämtlichen Anbietern und Betreibern von KI-Systemen die Verarbeitung von sensiblen Daten zu Zwecken der Erkennung und der Korrektur von Verzerrungen erlaubt, sofern angemessene hierin nor-

mierte Schutzmaßnahmen ergriffen wurden.
Zum Ausnahmetatbestand nach Art 9 Abs 2 lit k des Entwurfs zur DSGVO ist noch anzumerken, dass hier neue Rechtsbegriffe bzw. unklare Formulierungen gewählt werden. Der Begriff *„AI model"* („KI-Modell") wird weder in der KI-Verordnung noch in der DSGVO definiert. In der KI-VO ist der Begriff im Zusammenhang mit KI-Modellen mit allgemeinem Verwendungszweck (GPAI – general-purpose AI models) in den Art 51 ff KI-VO erwähnt. In technischer Hinsicht handelt es sich bei einem KI-Modell um einen Teil eines KI-Systems.
Auch der Begriff *„operation"* in Art 9 Abs 2 lit k und in Abs 5 des Entwurfs zur DSGVO ist unklar. Die KI-VO definiert lediglich den Begriff *„operator"* (zu Deutsch: „Akteur:in") in deren Art 3 Z 8 und subsumiert darunter sämtliche in der KI-VO adressierte Handelnde. Sollte eine derartige Auslegung auch in der DSGVO angedacht sein, so handelt es sich hierbei um eine viel zu weite und uE unzulässige Ausnahme vom Verbot der Verarbeitung sensibler Daten.

Die Ergänzung, dass sensible Daten für Zwecke der Entwicklung und des Betriebs eines KI-Systems oder -Modells verarbeitet werden können, lässt zudem befürchten, dass zukünftig vermehrt KI-Systeme eingesetzt werden, da sensible personenbezogene Daten damit leichter verarbeitet werden dürfen. Die Artikel-29-Datenschutzgruppe hat zutreffend darauf hingewiesen, dass gerade der Missbrauch sensibler Daten gravierendere Konsequenzen für die Grundrechte auf Privatsphäre und Nichtdiskriminierung haben kann, die irreversibel und langandauernd für das betroffene Individuum sein können (hohes Schadens- und Missbrauchspotential). Gerade im Kontext der Beschäftigung oder Betriebsratstätigkeit fällt eine Vielzahl an sensiblen Daten an, an welchen Arbeitgeber:innen aus verschiedenen Gründen ein großes Interesse an der Verwendung solcher Informationen haben können (beispielsweise bei Rückkehrgesprächen, Ursachenforschung bei Krankenständen, Gesundheits- und Krankenstandsdaten einzelner Arbeitnehmer:innen, Gewerkschaftszugehörigkeit oder Fehlzeiten). Und auch im Konsument:innenalltag finden sich von der Smartwatch bis zur Bestellung von medizinischen Produkten, politischen Schriften oder dem Aufruf einschlägiger Websites, die tracken, sensible Daten. Sie könnten in weiterer Folge aggregiert und von einem KI-System genutzt werden, um beispielsweise individuelle Preise, manipulative Techniken, die eine „Schwäche" ausnutzen etc, zu schaffen. Diese Daten müssen auch weiterhin einem besonders hohen Schutz unterliegen, weshalb diese vorgesehene Ergänzung klar abzulehnen ist.

Gegen den Ausnahmetatbestand des neu geschaffenen **Art 9 Abs 2 lit l** des Entwurfs zur DSGVO, wonach die Verarbeitung von biometrischen Daten erlaubt ist, sofern dies zu Zwecken der Bestätigung der Identität des Betroffenen erforderlich ist und die alleinige Kontrolle über die biometrischen Daten oder die Mittel zur Verifizierung beim Betroffenen liegt, bestehen aus Sicht der AK keine Einwände.

- **Art 12 DSGVO – Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person**

Art 12 DSGVO regelt die transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person und verweist dabei auf die verpflichtenden Informationen nach den Art 13 und 14 DSGVO und auf die Mitteilungen nach Art 15 bis 22 sowie Art 34 DSGVO, sohin auf die Betroffenenrechte wie zB das Auskunftsrecht nach Art 15 DSGVO.

Art 12 Abs 5 DSGVO soll nach dem KOM-Vorschlag um den Zusatz *„or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data (…)"* ergänzt werden, wonach ein Antrag auf Auskunftserteilung als offenkundig unbegründet abgelehnt werden kann, wenn die betroffene Person das durch diese Verordnung verliehene Recht für andere Zwecke als den Schutz ihrer personenbezogenen Daten missbraucht.

Dieser Zusatz schwächt Betroffene erheblich in ihrer Rechtsposition. Das allgemeine Auskunftsrecht ist **das zentrale Betroffenenrecht**. Seine herausgehobene Stellung zeigt sich in Art 8 Abs 2 Satz 2 GRCh, der dieses Recht ausdrücklich gewährleistet sowie in der Rechtsschutzgarantie von Art 47 GRCh. Jede (auch nur denkmögliche) Einschränkung dieses Rechts führt zu einer unzulässigen Aushöhlung grundrechtlicher Bestimmungen und ist daher bereits aus diesem Grund abzulehnen.

Zu befürchten ist, dass diese geplanten Änderungen insbesondere für Arbeitnehmer:innen als Betroffene in einem Arbeitsverhältnis mit dem dort immanent vorherrschenden Machtungleichgewicht, und sohin Informationsungleichgewicht, einen erheblichen Nachteil darstellen. In der Praxis wird dies auf eine massive Schlechterstellung ihrer Rechtsposition hinauslaufen. Durch den Einsatz moderner Technologien werden immer mehr Daten über Arbeitnehmer:innen erhoben, gesammelt und technisch weiterverarbeitet, verknüpft und ausgewertet. Dies darf nicht ohne entsprechende Information bzw. Auskunft an Betroffene erfolgen. Das allgemeine Auskunftsrecht ist ein für Arbeitnehmer:innen zentrales Betroffenenrecht, die Rechtmäßigkeit einer Datenverarbeitung durch den:die Arbeitgeber:in als Verantwortliche:n zu kontrollieren, Verstöße gegen den Beschäftigtendatenschutz zu erkennen oder Überwachung aufzudecken. Dieses Recht ist auch die Grundlage, um an eine Kopie ihrer Daten, wie zum Beispiel Unterlagen zu Entgeltberechnungen, Leistungsdaten,

interne Bewertungen über ihre Person, sie betreffende Dokumente, oder an einen sie betreffenden Schriftverkehr, zu gelangen. Der Zugang zu den eigenen Daten muss gerade in einem derartigen Abhängigkeitsverhältnis gewahrt bleiben und darf nicht der Einschränkung, dass dieses Recht für „Zwecke des Datenschutzes" verwendet werden muss, unterworfen werden.

Auch im Konsument:innenalltag ist das Auskunftsrecht oft die einzige, auch aufgrund von gesetzlichen Fristen gegenüber Verantwortlichen sanktionierbare Möglichkeit, beispielsweise interne und nicht gerechtfertigte Fremdzugriffe auf die eigenen Daten, wichtige Gesprächsnotizen im Rahmen eines Telefonats oder Vertragsunterlagen zu erhalten. Bei ausbleibender Erfüllung des Auskunftsrechts ist dieses mit dem kostenlosen Beschwerdeverfahren weiter verfolgbar, sodass in einem Machtungleichgewicht die Position des Betroffenen „gestärkt" wird. Im Zusammenhang damit gibt es auch schon einschlägige Rechtsprechung, was eine zulässige Auskunft oder Datenkopie ist, oder nicht. Die solcher Hand für Betroffenen gewonnene schrittweise Rechtssicherheit würde mit der vorgeschlagenen Änderung verloren gehen und sie nicht nur datenschutzrechtlich, sondern auch im Rahmen von zivilrechtlichen Verfahren, Gleichbehandlungskonflikten, im Nachweis von Diskriminierung etc. schwächen.

Der Unionsgesetzgeber hat selbst in Art 1 Abs 2 DSGVO festgelegt, dass die DSGVO alle Grundrechte schützt. Die DSGVO muss es betroffenen Menschen weiterhin ermöglichen, ihre Rechte und Interessen auf der Grundlage von Informationen über sich selbst zu verteidigen, und diejenigen, die Macht haben, dazu zu zwingen, gegenüber denen Rechenschaft abzulegen, die ihrer Autorität unterliegen.

Die Ausübung des Auskunftsrechts muss daher weiterhin im Einklang mit der Rechtsprechung des EuGH gewährleistet sein. Der EuGH hat in seiner Entscheidung vom 26.10.2023, C-307/22 klargestellt, dass die Auskunftsverpflichtung auch dann besteht, wenn der betreffende Auskunftsantrag mit einem anderen als den in der DSGVO genannten Zwecken begründet wird. Ein Auskunftsbegehren ist also nicht „offenkundig unbegründet" oder rechtsmissbräuchlich, wenn damit datenschutzfremde Ziele (wie Beschaffung von Beweismaterial für eine spätere Prozessführung) verfolgt werden.

Nach der Rechtsprechung des EuGH darf ein Zweck, der nichts mit dem Datenschutz zu tun hat, der Ausübung des Auskunftsrechts daher nicht von vornherein entgegenstehen. Der vorgeschlagene Einschub in Art 12 Abs 5 des Entwurfs zur DSGVO ist sohin auch im Lichte der Rechtsprechung des EuGH entschieden abzulehnen.

Auch der letzte eingeschobene Satz, wonach Verantwortliche darlegen müssen, dass der Antrag offenkundig unbegründet ist oder dass es vernünftige Gründe zu vermuten gibt, dass der Antrag exzessiv ist, ist aus Sicht der AK abzulehnen. Die Verweigerung des Auskunftsrechts des Betroffenen im Falle einer exzessiven Ausübung der Anfrage ist bereits nach geltendem Recht möglich. Nunmehr soll aber für die Beurteilung, ob die Ausübung exzessiv ist, nach dem Entwurf der Beweismaßstab herabgesenkt werden, wonach die bloße Vermutung der exzessiven Ausübung genügen soll.

Die vorgeschlagenen Änderungen für Art 12 Abs 5 des Entwurfs zur DSGVO sind daher zur Gänze abzulehnen, da sie entgegen der Ankündigung der Kommission keinesfalls bloß technischer Natur sind, sondern das Auskunftsrecht als das zentrale Betroffenenrecht erheblich und ohne Not einschränken.

- **Art 13 DSGVO – Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person**

Art 13 DSGVO regelt die Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person („Datenschutzerklärung"). Sie sind für Betroffene ein wichtiger und transparenter Hinweis darüber, was mit ihren Daten geschieht und wie sie ihre Rechte geltend machen können. So haben Verantwortliche nach Art 13 Abs 1 DSGVO zB über ihren Namen und ihre Kontaktdaten, aber auch die Kontaktdaten der Datenschutzbeauftragten, die Zwecke der Verarbeitung der personenbezogenen Daten sowie die Rechtsgrundlage für die Verarbeitung zu informieren. Art 13 Abs 2 DSGVO sieht eine Information unter anderem über die Speicherdauer sowie über das Bestehen des Auskunftsrechts und des Rechts auf Berichtung oder Löschung vor. Auch über eine beabsichtigte Zweckänderung haben Verantwortliche nach Art 13 Abs 3 DSGVO zu informieren. In der Praxis kommt dieser „Datenschutzerklärung" große Bedeutung zu, weil sie zB bei Konsument:innen aufkommende Fragen über den Zeitpunkt der Löschung ihrer Daten beantwortet.

Art 13 Abs 4 DSGVO soll nach dem KOM-Entwurf nun umformuliert werden. Waren bisher die Absätze 1, 2 und 3 des Art 13 DSGVO nicht anwendbar, wenn der Betroffene die Informationen bereits hat, so sieht die Kommission nun unter bestimmten Bedingungen ein weiter gefasstes Absehen dieser Informationserteilungspflicht vor.

Wurden die personenbezogenen Daten in einem „genauen und umschriebenen (Vertrags-)Verhältnis" (zu Englisch: „*in the context of a clear and circumscribed relationship*") über eine „nicht-datenintensive Aktivität" (zu Englisch: „exercising an activity that is

not data-intensive“) verwendet und gibt es „vernünftige Gründe, anzunehmen“ (zu Englisch: *„reasonable grounds to assume“*), dass die betroffene Person bestimmte Informationen, nämlich die Kontaktdaten der Verantwortlichen und ggf deren Vertreter und den Verarbeitungszweck samt Rechtsgrundlage für die Verarbeitung, bereits hat, so müssen diese Informationen nach dem Vorschlag der Kommission nicht erteilt werden. Diese Informationspflicht entfällt hingegen dann nicht, wenn Verantwortliche einem Dritten oder Kategorien von Dritten oder an einen Drittstaat übermitteln, oder wenn die Daten einer automatisierten Entscheidungsfindung, inkl. Profiling zugeführt werden oder die Verarbeitung dazu geneigt ist, zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen zu führen.

Die Kommission verwendet hier gleich mehrere unbestimmte Gesetzesbegriffe, die die Rechtsanwendung unnötig erschweren. So ist etwa unklar, was unter einem „klaren und umschriebenen (Rechts-)Verhältnis“ oder einer „nicht-datenintensiven Aktivität“ zu verstehen ist. Auch der Hinweis, dass die bloße Annahme der Verantwortlichen ausreicht, diese Informationen nicht zu erteilen, ist unklar und kann in der Praxis dazu führen, dass diese Vermutung schnell und leicht als Vorschub für die Nichterteilung von eben diesen Informationen herangezogen wird.

Die Ausnahme *„there are reasonable grounds to assume that the data subject already has the information“* ist vage und subjektiv, was zu unterschiedlichen Interpretationen und Anwendungsmöglichkeiten durch Arbeitgeber:innen führen kann. Arbeitnehmer:innen könnten dadurch über Daten, die über sie verarbeitet werden, nicht ausreichend informiert werden. Gerade im Kontext eines Arbeitsverhältnisses sind Arbeitnehmer:innen oft nicht in der Lage, alle personenbezogenen Daten nachzuvollziehen, die von ihren Arbeitgeber:innen erhoben und verarbeitet werden, da diese aus verschiedenen Quellen stammen können, wie beispielsweise Personalakten, Leistungsbewertungen oder Kommunikationsprotokollen. Die internen Prozesse zur Verarbeitung von personenbezogenen Daten können komplex und für Arbeitnehmer:innen, insbesondere in Betrieben ohne Betriebsrat undurchsichtig sein, insbesondere wenn keine klare und umfassende Information bereitgestellt wird. Arbeitnehmer:innen haben möglicherweise nicht die gleichen Informationsquellen wie Arbeitgeber:innen und können dadurch benachteiligt werden, wenn angenommen wird, dass sie bereits über die notwendigen Informationen verfügen. Wenn weniger Transparenz bezüglich der Verarbeitung personenbezogener Daten besteht, könnten Arbeitnehmer:innen ihre Rechte gemäß DSGVO (wie das Recht auf Auskunft und das Recht auf Berichtigung) weniger effektiv ausüben.

Für Konsument:innen sind die vollständig erteilten Informationspflichten auch ein Vehikel, das darüber entscheidet, ob sie überhaupt mit einem Unternehmen/Verantwortlichen in eine Beziehung treten wollen. Unabhängig davon zeigt die Praxis, dass es aktuell ein Informationsdefizit gibt, weil Verantwortliche Ihre Kund:innen schlichtweg nicht über die Datenverarbeitungen informieren. Das geschieht auf Kosten der Betroffenen, die nicht wissen, was mit ihren Daten geschieht. Doch gerade eine vollständige Datenschutzerklärung hilft auch Unternehmen, sich ihrer eigenen Datenverarbeitung bewusst zu werden und richtige „technische und organisatorische Maßnahmen“ zum Schutz ihrer Daten zu ergreifen. In einer digitalen Gesellschaft ist das essenziell, da nur dadurch richtige Vorkehrungen vor Cyberattacken etc. ergriffen werden können. Diese Informationen sollten deshalb immer vorliegen und auch Konsument:innen offen gelegt werden, auch weil das zu einem „Wettbewerb des hohen Datenschutzes“ führen kann.

Diese zentralen Informationspflichten dürfen daher keinesfalls eingeschränkt werden. Betroffene benötigen jedenfalls die in Art 13 DSGVO normierten Informationen, ohne die die Ausübung ihrer Rechte erheblich erschwert wird. Diese vorgeschlagenen Änderungen sind daher strikt abzulehnen.

- **Art 22 – automatisierte Entscheidungen im Einzelfall einschließlich Profiling**

Art 22 Abs 1 und 2 DSGVO soll nach dem Entwurf der Kommission durch bloß einen Absatz 1 ersetzt werden. Technisch sei hier angemerkt, dass der Verweis in Art 22 Abs 3 DSGVO dann entsprechend korrigiert werden müsste.

Die Möglichkeit der automatisierten Entscheidungen aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten (lit b) und bei ausdrücklicher Einwilligung der betroffenen Person (lit c) ist wie bisher weiterhin möglich. Absatz 1 lit a, wonach die automatisierte Entscheidung für den Abschluss oder die Erfüllung des Vertrags erforderlich ist, wird nach dem KOM-Entwurf zur DSGVO jedoch dahingehend ergänzt, dass diese Erforderlichkeit insofern abgeschwächt bzw. de facto ausgehöhlt wird, als dass eine automatisierte Entscheidung unabhängig davon zulässig ist, ob die Entscheidung auch anders als durch alleinige automatisierte Entscheidung getroffen werden kann.

Dieser Zusatz in lit a (nunmehr des Art 22 Abs 1 des Entwurfs zur DSGVO) bedeutet eine Abkehr vom derzeit mit Art 22 Abs 1 DSGVO bestehenden generellen Verbot einer ausschließlich automatisierten Entscheidung mit rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung (mit Ausnahmen im derzeit geltenden Art 22 Abs 2 DSGVO), was aus Sicht der AK jedenfalls abzulehnen ist.

Ist derzeit die Erforderlichkeit anhand der Vertragsziele im konkreten Einzelfall zu prüfen und musste die automatisierte Entscheidung demnach objektiv notwendig sein, so soll nach dem Entwurf eine solche Entscheidung auch dann zulässig sein, wenn sie anders als automatisiert getroffen werden kann. Damit ist der automatisierten Entscheidung im Zusammenhang mit dem Vertragsabschluss bzw. der Vertragserfüllung Tür und Tor geöffnet. Auf eine tatsächliche Erforderlichkeit im Sinne einer tatsächlichen Notwendigkeit kommt es nach dem Entwurf eben gerade nicht mehr an, was aus Sicht der Betroffenen entschieden abzulehnen ist.

So soll auch zukünftig zB im Arbeitsverhältnis immer zu berücksichtigen sein, ob nicht auch eine weniger eingriffsintensive Datenverarbeitung der Zweckerreichung führt. Betroffene müssen auch weiterhin das uneingeschränkte Recht haben, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden.

Die AK spricht sich daher klar für eine Beibehaltung der derzeitigen Regelung in Art 22 Abs 1 und 2 DSGVO aus.

- **Art 33 DSGVO – Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde**

Art 33 Abs 1 DSGVO soll laut dem Vorschlag der Kommission in zweierlei Hinsicht geändert werden: Die Meldung der Datenschutzverletzung hat nur noch bei hohem Risiko (anstelle von Risiko generell) für die Rechte und Freiheiten natürlicher Personen zu erfolgen und die Frist für die Meldung wurde von 72 Stunden auf 96 Stunden erhöht.

Die AK spricht sich gegen die vorgeschlagenen Änderungen aus. Für eine Erhöhung des Risikoniveaus als Auslöser für die Meldepflicht und für eine Verlängerung der ohnehin bereits sehr langen Frist bestehen keine sachliche Rechtfertigung und auch keine evidenzbasierte Notwendigkeit. Die vorgeschlagenen Änderungen lassen auch nachteilige Folgen für Betroffene wie zB Arbeitnehmer:innen und Verbraucher:innen und ihre Interessenvertretungen befürchten: Damit einher gehen weniger Transparenz, geringere Handlungs- und Mitbestimmungsmöglichkeiten – auch in der Zusammenarbeit mit der Datenschutzbehörde und/sowie die Erschwerung der Aufdeckung von Missständen.

Die Meldepflicht bereits im Falle eines Risikos für die Rechte und Freiheiten natürlicher Personen muss bestehen bleiben, da – wie Erwägungsgrund 85 zur DSGVO ausführt – die Verletzung des Schutzes personenbezogener Daten einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen kann, weshalb Verantwortliche wie bisher hier unverzüglich (mit einer Maximalfrist von 72 Stunden) die Aufsichtsbehörde über diese Verletzung zu unterrichten haben. Datenschutzbehörden sollen doch frühzeitig handeln und Abhilfemaßnahmen sollen rasch getroffen werden.

Ferner gibt es keinen Grund, bestehende Rechtsentwicklung in diesem Bereich auszuhöhlen und zu verwässern. Es gibt beispielsweise Leitlinien zum Thema oder die Aufsichtsbehörden stellen Formulare zur Verfügung, die eine Meldung niederschwellig ermöglichen. Welchen Nutzen eine Nivellierung nach unten in diesem Bereich haben soll, erschließt sich nicht, denn gerade eine ‚*Data Breach*'-Meldung kann der Aufsichtsbehörde möglicherweise seine Systematik zeigen, die es gemeinsam mit den Verantwortlichen zu beseitigen gilt. Das kann insbesondere dabei helfen, Cybercrime oder strukturelle Mängel, die nachteilig für Betroffene und die Gesellschaft sind, rechtzeitig zu erkennen und zu beseitigen.

- **Art 35 DSGVO – Datenschutz-Folgenabschätzung**

Die geplante Harmonisierung der Durchführung von Datenschutz-Folgenabschätzungen (DSFA), indem auf EU-Ebene eine einheitliche Liste von Verarbeitungsoperationen vorgelegt wird, die eine DSFA erfordern und nicht erfordern, verbessert auch die Rechtssicherheit (va in grenzüberschreitenden Sachverhalten) und somit ebenfalls deren Einhaltung durch Verantwortliche. Hinzuweisen ist allerdings, dass die Abschaffung nationaler Listen (siehe Verordnungen der DSB in Österreich) dazu führen könnte, dass in Zukunft spezifische nationale Gegebenheiten (Bestehen betrieblicher Interessenvertretungen, kollektiver Normen wie etwa Betriebsvereinbarungen) und Risiken nicht ausreichend berücksichtigt werden. Dass der Europäische Datenschutzausschuss (EDPB) diese Listen sowie Vorschläge für die Methodik der Durchführung der DSFA zu erstellen hat, wird begrüßt. Sehr kritisch gesehen wird allerdings, dass die EU-Kommission befugt ist, diese abzuändern bzw. zu „aktualisieren". Es wäre wünschenswert, wenn dies in Händen des unabhängigen EDPD bliebe. Auch erscheint das Zeitintervall der Überprüfung mit drei Jahren angesichts der rasanten technologischen Entwicklungen als zu lange. Durch eine laufende Beobachtung und Evaluierung sollen neue Risiken besser zeitnah adressiert werden.

- **Art 88a DSGVO – Verarbeitung von personenbezogenen Daten in Endeinrichtungen von natürlichen Personen**

Die neu einzufügenden Art 88a und Art 88b DSGVO sind in Zusammenschau mit der von der Kommission vorgeschlagenen Ergänzung in Art 5 Abs 3 der Datenschutzrichtlinie für elektronische Kommunikation („e-privacy-RL"; siehe Artikel 5 des KOM-Vorschlags) zu lesen und betreffen die sog. „cookie"-Regelung.

Die Kommission schlägt vor, die Verarbeitung von nicht-personenbezogenen Daten in Art 5 Abs 3 der e-privacy-RL zu belassen und die Verarbeitung von personenbezogenen Daten in Endeinrichtungen in einen neuen Art 88a der DSGVO einzubetten.

Während Art 5 Abs 3 der e-privacy-RL um einen Unterabsatz ergänzt wird, wonach die Bestimmung des Art 5 Abs 3 der e-privacy-RL nicht anwendbar ist, wenn der Teilnehmer oder Nutzer eine natürliche Person ist und die Speicherung oder der Zugriff auf Informationen eine Verarbeitung von personenbezogenen Daten darstellt oder dazu führt, werden mit Art 88a und Art 88b des Vorschlags zur DSGVO umfassende Regelungen für die Verarbeitung von personenbezogenen Daten in Endeinrichtungen von natürlichen Personen geschaffen.

Nach Art 88a Abs 1 des Vorschlags der Kommission zur DSGVO soll die Speicherung von oder der Zugriff auf bereits gespeicherte personenbezogene Daten in Endeinrichtungen einer natürlichen Person nur dann zulässig sein, wenn die Person ihre Einwilligung erteilt hat. Nach Abs 2 leg cit ist die Speicherung oder der Zugriff auf personenbezogene Daten in Endeinrichtungen auch auf der Basis von Unions- oder Mitgliedstaatsrecht unter Einhaltung der Bedingungen des Art 6 DSGVO zur Erreichung der in Art 23 Abs 1 DSGVO normierten Ziele zulässig. Damit ist etwa die Datenverarbeitung zu Zwecken der nationalen Sicherheit, bei entsprechender gesetzlicher Grundlage, zulässig.
Art 88a Abs 3 des Entwurfs zur DSGVO regelt sodann die Zulässigkeit der Verarbeitung von personenbezogenen Daten in Endeinrichtungen – sofern notwendig – **ohne** Zustimmungen der betroffenen Person in vier aufgelisteten Varianten: zur Übertragung einer elektronischen Nachricht über ein elektronisches Kommunikationsnetzwerk (lit a); um einen ausdrücklich vom Datensubjekt gewünschten Dienst zur Verfügung zu stellen (lit b); um aggregierte Informationen über die Verwendung eines Online-Dienstes zur Erfassung der Zielgruppe zu schaffen, sofern dies von Verantwortlichen dieses Online-Dienstes allein für die eigene Verwendung erfolgt (lit c); um die Sicherheit des Dienstes der Verantwortlichen, der von Betroffenen angefordert wurde oder wenn die Endeinrichtung für die Erbringung eines solchen Dienstes verwendet wird (lit d).
Waren die beiden ersten Varianten bereits in der Anwendung des derzeit geltenden Art 5 Abs 3 der e-privacy-RL bekannt, so schaffen die beiden letzten Varianten neue Rechtmäßigkeitsgründe für die Verarbeitung von personenbezogenen Daten in Endeinrichtungen ohne Zustimmung der betroffenen Person.

Art 88a Abs 4 des Entwurfs zur DSGVO schafft sodann weitere Regelungen im Falle des Vorliegens einer Einwilligung der betroffenen Person zur Speicherung oder zum Zugriff auf personenbezogene Daten in Endeinrichtungen: Die betroffene Person muss die Einwilligung mit einem „single-click button" oder ähnlichem verweigern können (lit a); Verantwortliche müssen für eine bestimmte Zeitspanne, in der sie sich auf die Einwilligung rechtmäßig berufen können, keine neuerliche Anfrage zur Einwilligung stellen (lit b); im Falle der Verweigerung der Einwilligung dürfen Verantwortliche für zumindest 6 Monate keine weitere Anfrage zur Einwilligung für denselben Zweck stellen (lit c). Nach Art 88a Abs 4 letzter Unterabsatz wird auch die Weiterverarbeitung von personenbezogenen Daten unter Anwendung der eben erwähnten Bestimmungen subsumiert.

Auf das Arbeitsverhältnis umgelegt, ermöglicht die Regelung damit Zugriffe des:der Arbeitgeber:in auf personenbezogene Daten der Arbeitnehmer:innen auf Smartphone, Laptop, IoT Geräte etc, die diese im Rahmen des Arbeitsverhältnisses verwenden. Das birgt in der Praxis die erhöhte Gefahr, dass – va in betriebsratslosen Betrieben – zukünftig immer mehr Prüfwerkzeuge (-systeme) ohne Zustimmung des:der Arbeitnehmer:in eingesetzt werden und bedeutet eine zusätzliche Verschlechterung ihrer Rechtsposition durch vermehrte Überwachungsrisiken. Art 88a Abs 1 des Entwurfs zur DSGVO widerspricht im Übrigen dem Art 6 DSGVO (die Verarbeitung auf Endgeräten kann auch auf andere Rechtsgrundlagen gegründet sein, als die Einwilligung). Auch der vorgeschlagene Abs 4 enthält Formulierungen, welche die klaren Vorgaben zur Rechtmäßigkeit der Verarbeitung in Art 6 DSGVO verwässern, womit Rechtsunsicherheit vorprogrammiert ist. Es erschließt sich auch nicht, weshalb es diese neuen Rechtmäßigkeitsgründe geben soll. Die darin genannten Zwecke sind ohne weiteres über Art 6 DSGVO erreichbar.

Die vorgeschlagene Regelung lässt auch außer Acht, dass die Verarbeitung von Daten auf Endgeräten nicht in einem geschlossenen System vor sich geht, sondern dazu führt, dass unzählige Dritte die personenbezogenen Daten von Betroffenen mitauslesen können, weil Verantwortliche beispielsweise auf bekannte Website-/App-Analyse-Tools oder Programmcodes zurückgreifen bzw. externe Cloud-Services nutzen. Diese wiederum aggregieren damit ihrerseits neue Daten („(Cross-Site-)Tracking/Profiling") und können so – weit über das Endgerät hinausgehende - Profile von Nutzer:innen generieren. Damit sind gläserne Bürger:innen die Regel. Es ist nicht nachvollziehbar, weshalb es dafür keine strenge Rechtfertigung nach Art 6 DSGVO brauchen soll, denn der vorliegende Vorschlag ermöglicht es, dass Verantwortliche sich einfachheitshalber der neuen Ausnahmetatbestände bedienen, ohne eine Einwilligung einholen zu müssen.

Die vorgeschlagene Regelung berücksichtigt auch nicht den Umstand, dass die Endeinrichtungen auch

von mehreren Personen genutzt werden bzw. dass sich auf ihr Informationen über Dritte befinden können, die keinerlei Information über die Verarbeitung ihrer Daten haben. Das untergräbt Art 5 Abs 2 DSGVO, der die Rechenschaftspflicht bei den Verantwortlichen sieht. Mit dem Vorschlag der EK wird impliziert, dass die natürliche Person eine Einwilligung dieser Dritten für die Datenverarbeitungen hat.

Der gegenständliche Entwurf des Art 88a geht weit über die Vorgängerbestimmung in Art 5 Abs 3 e-privacy-RL hinaus. Für eine derart weitreichende Regelung in Art 88a f des Vorschlags zur DSGVO besteht keine Notwendigkeit. Art 88a Abs 3 lit c und lit d des Entwurfs schaffen allzu weitreichende Ausnahmen für die Datenverarbeitung; auch die Weiterverarbeitung von personenbezogenen Daten soll nach Art 88a Abs 4 letzter Unterabsatz ohne Not erleichtert werden. Das Verhältnis zu Art 7 Abs 3 DSGVO bleibt ebenfalls unklar.

Diese erweitere Regelung in Art 88a DSGVO ist aus Sicht der AK jedenfalls abzulehnen; die derzeitige Bestimmung des Art 5 Abs 3 der e-privacy-RL sollte aus Sicht der AK bestehen bleiben.

- **Art 5 Abs 3 der e-privacy-RL – einstige „cookie"-Bestimmung**

Art 5 Abs 3 der e-privacy-RL regelte bislang, dass Konsument:innen im Falle der Speicherung oder der Zugriffs auf Informationen, die im Endgerät gespeichert sind, klare und umfassende Informationen insbesondere über die Zwecke der Verarbeitung erhalten und auf das Recht hingewiesen werden, diese Verarbeitung zu verweigern.

Diese Bestimmung wird nun auf nicht-personenbezogene Daten eingeschränkt. Tatsächlich sind nicht-personenbezogene Daten aufgrund dieser Bestimmung nun aber besser geschützt als personenbezogene Daten in und von Endgeräten durch den neu vorgeschlagenen, sehr weit gefassten Art 88a DSGVO.

Aus Verbraucher:innensicht sollte der bestehende Art 5 Abs 3 e-privacy-RL daher bestehen bleiben. Für eine Aufgliederung in Art 88a DSGVO und Art 5 Abs 3 e-privacy-RL besteht keine Notwendigkeit; sie dient auch nicht der Rechtsklarheit. Vielmehr ermöglicht sie es Verantwortlichen, sich nicht an die Grundsätze der Datenminimierung und des ‚privacy by default' halten zu müssen. Durch die neue Lösung wird ein in der Praxis nicht funktionierendes System rechtlich „saniert" und laufende vorherrschende Rechtsverstöße auf eine legale Basis gebracht. Dabei gibt es bereits zahlreiche Rechtssprüche, die sich mit der richtigen Ausgestaltung von Cookie-Bannern beschäftigen. Ebenso gibt es einen Bericht der Arbeit der „Cookie Banner Taskforce" des Europäischen Datenschutzausschusses. All das hilft Verantwortlichen, ihre Datenverarbeitung richtig auszugestalten.

- **Art 88b – automatisierte und maschinenlesbare Angaben zu den Entscheidungen der betroffenen Person hinsichtlich der Verarbeitung personenbezogener Daten in den Endgeräten natürlicher Personen**

Art 88b des Entwurfs zur DSGVO schafft die Verpflichtung, dass Verantwortliche auf ihren Online-Schnittstellen betroffenen Personen die Möglichkeit geben sollen, ihre Einwilligung automatisiert und maschinenlesbar zu erteilen, sofern die Voraussetzungen für eine Einwilligung nach der DSGVO vorliegen (Art 88b Abs 1 lit a) bzw. die Anfrage zur Einwilligung und das Widerspruchsrecht nach Art 21 Abs 2 DSGVO automatisiert und maschinenlesbar abzulehnen bzw. auszuüben. Verantwortliche haben die getroffene Entscheidung zu respektieren (Art 88b Abs 2).

Für Mediendienste soll dies nach Art 88b Abs 3 des Entwurfs nicht anwendbar sein.

Die Kommission soll nach Abs 4 des Entwurfs zu Art 88b eine europäische Standardisierungsorganisation zur Erarbeitung von Standards für die Interpretation von maschinenlesbaren Angaben zu den Entscheidungen der betroffenen Person auffordern. Kleinunternehmen, die Webbrowser zur Verfügung stellen, sind von dieser Bestimmung nach dem vorgeschlagenen Art 88b Abs 6 ausgenommen.

Wiewohl automatisierte und maschinenlesbare Angaben zu Entscheidungen der betroffenen Person hinsichtlich der Verarbeitung personenbezogener Daten grundsätzlich zu begrüßen sind, ist die vorgeschlagene Bestimmung in Teilen vage, zu weit bzw. unklar. Unklar ist hier etwa der Anwendungsbereich der Bestimmung, ob diese Möglichkeit also nur im Bereich des Art 88a des Vorschlags gelten soll oder für sämtliche Einwilligungen. Unbeantwortet bleibt auch, ob bzw. wie sichergestellt ist, dass es sich bei einer automatisierten und maschinenlesbaren Einwilligung um eine informierte Willensbekundung im Sinne des Art 4 Z 11 DSGVO handelt. Es ist auch unverständlich, ob die Zurücknahme einer Einwilligung ebenfalls automatisiert und maschinenlesbar ermöglicht werden soll. Auch das Verhältnis zu Art 21 Abs 5 DSGVO ist ungeklärt. Auch der bloße Respekt einer getroffenen Entscheidung in Art 88b Abs 2 des Entwurfs ist eine zu weich formulierte Bestimmung. Soll die Entscheidung verbindlich sein, so sind die Verantwortlichen zur entsprechenden Berücksichtigung zu verpflichten.

Diese Bestimmung bedarf daher noch weiterer (gesetzlicher) Klarstellungen bzw. Einschränkungen

und kann in der vorgeschlagenen Form nicht unterstützt werden.

- **Art 88c DSGVO – Verarbeitung im Zusammenhang mit der Entwicklung und dem Betrieb von KI**

Mit Art 88c DSGVO sowie den Erwägungsgründen 30f. will die Kommission das Trainieren (die Entwicklung) und den Betrieb von KI mit personenbezogenen Daten auf ein berechtigtes Interesse stützen lassen, es sei denn, Unionsrecht oder nationales Recht erfordert explizit eine Einwilligung.

Diese Bestimmung schafft keine eigenständige Rechtmäßigkeitsgrundlage für die Datenverarbeitung, sondern soll im Zusammenhang mit der Entwicklung und dem Betrieb von KI neben Art 6 Abs 1 lit f DSGVO zur Anwendung gelangen.

Dieser Vorschlag räumt Arbeitgeber:innen die Möglichkeit ein, sich auf ein berechtigtes Interesse iSd Art 6 Abs 1 lit f DSGVO für die Verarbeitung personenbezogener Daten für das Entwickeln oder den Betrieb eines KI-Systems bzw. eines -Modells zu stützen und wirft insbesondere im Kontext eines Arbeitsverhältnisses erhebliche Bedenken auf. Diese Bestimmung und die Änderung des Art 9 Absatz 2 DSGVO sowie entsprechende Bestimmungen in der KI-VO sind nicht aufeinander abgestimmt und werfen eine Unmenge an Fragen auf.

Im Arbeitsverhältnis besteht ein strukturelles Machtungleichgewicht zwischen Arbeitgeber:innen und Arbeitnehmer:innen. Arbeitnehmer:innen sind häufig gezwungen, ihre Daten preiszugeben, um ihre Beschäftigung nicht zu gefährden. Die geplante Änderung könnte dazu führen, dass Arbeitgeber:innen personenbezogene Daten ihrer Beschäftigten verarbeiten, um KI-Systeme zu entwickeln oder zu betreiben, ohne dass die Betroffenen eine echte Möglichkeit haben, sich dagegen zu wehren. Dies könnte die Rechte und Freiheiten der Arbeitnehmer:innen erheblich beeinträchtigen. KI-Systeme sind für die Arbeitnehmer:innen und ihre Vertretungen oft komplex und schwer nachvollziehbar. Die geplante Änderung könnte dazu führen, dass Arbeitnehmer:innen noch weniger Kontrolle über ihre Daten haben und nicht ausreichend informiert werden, wie ihre Daten verwendet werden. KI-Systeme, die auf personenbezogenen Daten basieren, könnten dazu verwendet werden, Arbeitnehmer:innen zu überwachen, ihre Leistung zu bewerten oder ihr Verhalten zu analysieren. Dies birgt das Risiko einer umfassenden Kontrolle und Überwachung am Arbeitsplatz, die die Privatsphäre der Beschäftigten massiv einschränken könnte. KI-Modelle sind anfällig für Verzerrungen und Diskriminierung, insbesondere wenn sie auf fehlerhaften oder unausgewogenen Datensätzen trainiert werden. Die Verarbeitung personenbezogener Daten von Arbeitnehmer:innen könnte dazu führen, dass diskriminierende Entscheidungen getroffen werden. Dies könnte die Chancengleichheit am Arbeitsplatz gefährden. Es sollte die Mitbestimmung durch die Belegschaft bei der Einführung von KI-Systemen am Arbeitsplatz, inklusive Zugang zu Daten, Modellen und Entscheidungslogiken sichergestellt sein.

Art 88c des Entwurfs enthält außerdem eine Reihe unbestimmter Formulierungen, deren Mehrwert angesichts der Vielzahl an unklaren Formulierungen äußerst fraglich ist. Bereits jetzt kann die Entwicklung und der Betrieb auf ein berechtigtes Interesse im Sinne des Art 6 Abs 1 lit f DSGVO gestützt werden. Der Grundsatz der Datenminimierung und die Transparenzpflichten gegenüber der betroffenen Person sind bereits nach geltendem Recht einzuhalten.

Art 88c des Entwurfs sollte daher nach Ansicht der AK ersatzlos gestrichen werden.

- **Ergänzende Regelung – Betroffenenrechte und Recht auf Erklärung**

Die DSGVO und die KI-VO bieten Rechtsschutz bei KI-basierten Entscheidungen. Die DSGVO normiert individuelle Betroffenenrechte, einschließlich des Rechts auf Information hinsichtlich Art 22 DSGVO, die KI-VO gewährt KI-spezifische Transparenz- und Informationspflichten.

Die Anwendungsbereiche der DSGVO und der KI-VO überlappen sich, dennoch sind KI-Systeme bzw algorithmische Entscheidungen nicht vollständig erfasst, u.a. wenn weder ein (Hochrisiko-)KI-System nach der KI-VO noch eine vollautomatisierte Entscheidungsfindung nach Art 22 DSGVO vorliegt. Betroffenen Personen stehen in solchen Fällen weder die entsprechenden Rechtsschutzmöglichkeiten nach der DSGVO noch nach der KI-VO zu. Ebenso gestaltet sich die Abgrenzung zwischen automatisierten, KI-gestützten und automationsunterstützten Entscheidungsprozessen in der Praxis oft schwierig, wodurch Systeme in einen rechtlichen „Graubereich" fallen können.

Diese Rechtsschutzlücke sollte behoben werden, insbesondere wenn durch neue Rechtsgrundlagen zum KI-Training in die Grundrechte betroffener Personen eingegriffen wird. Da KI-Systemen bzw. KI-basierten Entscheidungen immer ein Risiko für die informationelle Selbstbestimmung des Betroffenen innewohnt, sollte die Rechtsprechung des EuGH zum Recht auf Erklärung auf alle KI- Systeme bzw. algorithmische Systeme zur Entscheidungsfindung ausgeweitet werden. Eine ergänzende Bestimmung sollte Verantwortliche verpflichten, Information bzw. Auskunft über Logik und Tragweite von automatisierten bzw. KI-basierten Entscheidungen zu geben.

Vorschlag für Artikel 22a:
„Personen, die von einer Entscheidung betroffen sind, die der Verantwortliche auf der Grundlage der Ausgaben eines KI-Systems oder eines algorithmischen Systems zur automatisierten Entscheidungsfindung getroffen hat und die rechtliche Auswirkungen hat oder sie in ähnlicher Art erheblich auf eine Weise beeinträchtigt, die ihrer Ansicht nach ihre Gesundheit, ihre Sicherheit oder ihre Grundrechte beeinträchtigt, haben das Recht, vom Betreiber eine klare und aussagekräftige Erläuterung zur Rolle des KI-Systems im Entscheidungsprozess, zu den wichtigsten Elementen der getroffenen Entscheidung sowie aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zu erhalten."

Verordnung über künstliche Intelligenz (KI-VO)

Die Verordnung über künstliche Intelligenz (KI-VO) ist am 1.8.2024 in Kraft getreten, Geltungsbeginn ist zu großen Teilen der 2.8.2026. Sie wurde von der AK bereits umfassend für ihre Schwächen beim Grundrechtsschutz kritisiert, wie zum Beispiel angesichts des sehr eng gefassten Schadensbegriffs bei verbotenen KI-Praktiken (siehe Positionspapier aus Verbraucherschutzperspektive vom Jänner 2025). Die nun im Digital Omnibus Paket vorgeschlagenen Änderungen der KI-VO verschärfen diese Schieflage. Was sich als technische Anpassungen und Entbürokratisierungsmaßnahmen präsentiert, entpuppt sich bei genauerer Betrachtung als weitere Abschwächung der KI-VO. Die KI-VO droht zu einem Instrument zu verkommen, das seinen Schutzzweck verfehlt, noch bevor sie vollständig zur Anwendung kommt.

- **Erweiterte Ausnahmen für Small Mid-Cap Unternehmen (Art 1, 3, 11, 17, 57, 70, 95, 96, 99 KI-VO) bzw. für KMUs (Art 63 KI-VO)**

Die Europäische Kommission erweitert die Ausnahmeregelungen für kleine und mittlere Unternehmen („KMUs") auf mittelgroße Unternehmen. Dafür eingeführt werden die Definition von Kleinst-, kleines und mittleres Unternehmen („SME" bzw. „KMU") in Art 3 Abs 14a des Entwurfs zur KI-VO und die Definition von Small Mid-Cap Unternehmen („SMC") in Art 3 Abs 14b des Entwurfs zur KI-VO, entnommen aus dem Annex der Empfehlung (EU) 2025/1099 der Kommission. Als SMC gilt demnach ein Unternehmen mit bis zu 749 Mitarbeiter:innen, sofern entweder der Jahresumsatz 150 Millionen Euro oder die Jahresbilanzsumme 129 Millionen Euro nicht überschreitet. Erst wenn beide Finanzschwellen überschritten werden, fällt ein Unternehmen aus der SMC-Definition. Durch die Kopplung dieser Kriterien soll sichergestellt werden, dass unterschiedliche Geschäftsmodelle gleichermaßen erfasst werden, etwa ein Handelsunternehmen mit hohem Umsatz bei geringem Vermögen.

SMCs sollen die für KMU in der KI-VO bereits vorgesehenen Vereinfachungen ebenfalls eingeräumt werden. Das ist akkordiert mit den vorgeschlagenen Änderungen bei Art 30 Abs 5 DSGVO im 4. Omnibus-Paket und folgt den Politischen Leitlinien der Europäischen Kommission 2024-2029.

Der Adressat:innenkreis für Vereinfachungen würde sich damit erheblich erweitern, mit für Konsument:innen erheblichen Nachteilen: Mittelgroße Unternehmen haben besonders hohe Anteile in KI-relevanten Schlüsselindustrien. Dazu kommt, dass rund ein Viertel dieser Unternehmen keine eigenständigen mittelständischen Betriebe, sondern Tochtergesellschaften multinationaler Konzerne sind – die Hälfte davon mit Muttergesellschaften außerhalb der EU. Die im Annex von (EU) 2025/1099 definierten Kriterien für ein „eigenständiges Unternehmen" schaffen erhebliche Schlupflöcher: Beteiligungen durch Private Equity bleiben zum Beispiel unberücksichtigt, sofern diese nicht die Mehrheit der Stimmrechte halten oder formale Kontrolle ausüben. Im Gegensatz dazu gilt für Business Angels nach Punkt 3.4. des Anhangs zur Empfehlung (EU) 2025/1099 eine Obergrenze von 5 Millionen Euro. Das heißt: Ein Start-up mit 300 Mitarbeiter:innen, 5 Millionen Euro Business Angel-Finanzierung und professionellem Management-Team wird genauso behandelt wie ein klassischer Familienbetrieb mit 30 Mitarbeiter:innen ohne externe Finanzierung – obwohl die Ressourcen und das Know-how deutlich unterschiedlich sind. Während die gezielten Erleichterungen für KMUs in der KI-Verordnung eine Abwägung zwischen begrenzten Ressourcen kleiner Unternehmen und Schutzniveau darstellten, hebt die Ausweitung auf mittelgroße Unternehmen diesen Vorteil faktisch wieder auf.

In der KI-VO betreffen die ausgeweiteten Erleichterungen für SMCs vor allem zwei zentrale Bestimmungen: Die technische Dokumentation nach Art 11 und das Qualitätsmanagementsystemnach Art 17 KI-VO. Art 11 Abs 1 KI-VO gestatten derzeit die vereinfachte Darstellung der technischen Dokumentation nach Annex IV für KMU, einschließlich neu gegründeter Unternehmen. Art 17 Abs 2 KI-VO definiert, dass die Umsetzung eines in Abs 1 näher definierten Qualitätsmanagementsystems in einem angemessenen Verhältnis zur Größe einer Organisation des Anbieters erfolgen soll.

Der Vorschlag, die für KMU und Start-Ups vorgesehenen Vereinfachungen derart auf SMCs auszuweiten, ist aus mehrfacher Hinsicht abzulehnen: Die KI-VO als Produktsicherheitsrecht für Künstliche Intelligenz normiert nach dem Risiko des KI-Systems gestaffelte Anforderungen an Künstliche Intelligenz. Die von der

Kommission vorgeschlagenen Erleichterungen in der KI-VO für SMC entbehren jeglicher sachlicher Rechtfertigung, geht es in der KI-VO doch um Risikoverringerung und Schadensvermeidung, gemessen am Risiko des KI-Systems, nicht an der Unternehmensgröße. Die vorgeschlagenen Erleichterungen sind daher aus Betroffenensicht abzulehnen. Gerade Art 11 und Art 17 der KI-VO bilden zentrale Qualitätssicherungsinstrumente für Hochrisiko-KI-Systeme, die über Kreditwürdigkeit, Beschäftigungschancen, Sozialleistungsansprüche oder biometrische Identifikation entscheiden. Ein funktionierendes Qualitätsmanagementsystem und vollständige technische Dokumentation sind hier aus Sicht der AK besonders wichtig.

Die Verhältnismäßigkeitsklausel in Art 17 Abs 2 KI-VO und die vereinfachte Dokumentation nach Art 11 Abs 1, 2. Unterabsatz KI-VO setzen voraus, dass kleinere Organisationen strukturell nicht über die Kapazitäten großer Konzerne verfügen. SMCs verfügen typischerweise aber über hunderte Mitarbeitende und dedizierte Compliance-Abteilungen – eine Gleichstellung mit KMUs und Startups entbehrt sohin jeder sachlichen Grundlage.

Auch die vorgeschlagene Ergänzung in Art 99 KI-VO, wonach hinsichtlich der Sanktionen nunmehr auch auf die Interessen von SMCs Rücksicht zu nehmen ist, ist aus Sicht der AK abzulehnen.

Thematisch fügt sich hier auch die vorgeschlagene Änderung des Art 63 Abs 1 KI-VO, wonach nicht mehr Mikrounternehmen, sondern generell KMUs von den hier normierten Ausnahmen profitieren. Die AK spricht sich mangels sachlicher Rechtfertigung gegen eine derartige Ausweitung auf KMUs aus.

- **Art 4 KI-VO – KI-Kompetenz**

Art 4 KI-VO nimmt bereits in seiner geltenden Fassung einen unverbindlichen Ansatz zur KI-Kompetenz ein und verpflichtet Unternehmen lediglich, „nach besten Kräften" sicherzustellen, dass das Personal über ein „ausreichendes Maß" an KI-Kompetenz verfügt. Art 4 KI-VO ist eine Voraussetzung zur Erfüllung von Art 14 KI-VO, welcher die menschliche Aufsicht regelt. Ohne ein ausreichendes Maß an KI-Kompetenz ist die für Hochrisiko-KI verpflichtende menschliche Aufsicht jedenfalls nicht sicherzustellen.

Art 4 KI-VO ist auch wichtig, weil er eine der wenigen Verpflichtungen für nicht Hochrisiko-KI-Systeme in der KI-VO darstellt.

Die vorgeschlagene Änderung beabsichtigt allerdings, diese ohnehin minimale Verpflichtung zu einer bloßen Empfehlung zu degradieren: Die Kommission und die Mitgliedstaaten würden Anbieter und Betreiber lediglich „ermutigen", KI-Kompetenz bereitzustellen, anstatt diese zu fordern. Diese vorgeschlagene vage und unverbindliche Formulierung bedeutet nicht nur die Abschaffung der Verpflichtung für Anbieter und Betreiber, KI-Kompetenz zu gewährleisten, sondern auch, dass KI-Kompetenz für KI-Einführung und -Einsatz insgesamt keine Rolle spielen wird. Das ist aus gesellschaftlicher Sicht und aus Perspektive der Wettbewerbsfähigkeit negativ: Für Unternehmen ist KI-Kompetenz die Grundlage für Risikominimierung einerseits hinsichtlich der potenziell negativen Auswirkungen auf die Gesundheit, Sicherheit und Grundrechte zB der Arbeitnehmer:innen und andererseits hinsichtlich Haftung oder falscher Anwendung von KI-Systemen. Darüber hinaus ist KI-Kompetenz die Grundlage für die produktive KI-Nutzung. Die de facto Abschaffung dieser Verpflichtung widerspricht daher auch den strategischen Zielen der EU (bspw. Apply AI Strategie). Aus gesellschaftlicher Sicht ist KI-Kompetenz die Grundlage für die kollektive Kontrolle und Wahrung der demokratischen Werte. Anstatt der Abschaffung der Verpflichtung sollten im Gegenteil die Pflichten der Kommission und der Mitgliedstaaten zur Förderung der KI-Kompetenz ausgebaut werden.

Dieser Vorschlag ist aus Betroffenensicht daher abzulehnen. Für ein Produktsicherheitsrecht wie die KI-VO sollte die Sicherstellung, dass Bediener:innen kompetent im Umgang mit einem System sind, das absolute Minimum darstellen – nicht nur bei Hochrisiko-KI-Systemen. Art 4 KI-VO ist seit Februar 2025 anwendbar, ohne dass bisher dokumentierte Durchsetzungsfälle bekannt sind. In der Praxis werden Verstöße gegen die Kompetenzverpflichtung jedoch voraussichtlich erst dann sichtbar, wenn Hochrisiko-Systeme versagen und Untersuchungen unzureichende KI-Kompetenz als Ursache identifizieren. An diesem Punkt wird der Unterschied zwischen „Kompetenz sicherstellen" und „ermutigen, Kompetenz bereitzustellen" für Haftung und Verantwortlichkeit entscheidend sein.

Kompetente Beschäftigte, die gut auf die neuen Herausforderungen im Unternehmen vorbereitet sind und in die Planung der Digitalisierung eingebunden werden, erleichtern die Einführung und Anwendung von KI sowie die Umgestaltung interner Prozesse und Arbeitsabläufe. Die notwendige KI-Kompetenz ergibt sich direkt aus dem spezifischen Unternehmens- bzw. Organisationskontext und den dort eingesetzten KI-Technologien. Die Verantwortung für die Implementierung von KI-Systemen sowie deren Einsatzzwecke liegt bei den Unternehmen selbst und richtet sich auch nach deren strategischer Ausrichtung. Folglich muss auch die Entwicklung der notwendigen KI-Kompetenz innerhalb der Unternehmen erfolgen. Eine Übertragung dieser Aufgaben auf die Kommission oder ihre Mitgliedstaaten wäre nicht zielführend und würde den Zweck der Regelung verfehlen. Daher kann das Argument der

„zusätzlichen Compliance-Belastung" nicht überzeugen. Unternehmen profitieren selbst von der Verbesserung der Arbeitsprozesse, der Unterstützung durch KI-Technologien, der erhöhten Sicherheit im Umgang mit KI und dem Verständnis der eigenen Rechte und Pflichten im Kontext von KI-Anwendungen.

- **Art 4a des Entwurfs zur KI-VO – Verarbeitung besonderer Kategorien personenbezogener Daten zum Zweck der Erkennung und Korrektur von Verzerrungen**

Vorgesehen ist die Einführung eines neuen Artikels 4a KI-VO, der die Verarbeitung besonderer Kategorien personenbezogener Daten zum Zweck der Erkennung und Korrektur von Verzerrungen ('bias') erlauben soll. Während sich Art 4a Abs 1 des vorgeschlagenen Entwurfs zur KI-VO weitgehend mit Art 10 Abs 5 KI-VO deckt, weitet Art 4a Abs 2 nunmehr die Erlaubnis der Verwendung besonderer personenbezogener Daten für Anbieter:innen und Betreiber:innen sämtlicher KI-Systeme und -Modelle und Betreiber von Hochrisiko-KI-Systemen aus, soweit dies für die festgelegten Zwecke erforderlich ist.

Dies stellt eine massive Ausweitung der ursprünglich nur bei Hochrisiko-KI-Systemen vorgesehenen Ausnahme für die Verarbeitung besonderer Kategorien personenbezogener Daten dar und ist aus Sicht der AK jedenfalls abzulehnen. Art 10 Abs 5 KI-VO sollte unverändert bestehen bleiben.

- **Streichung der Registrierungsverpflichtung für KI-Systeme nach Annex III, die aus Unternehmenssicht keine Hochrisiko-KI-Systeme sind (Art 6 Abs 4, Art 49 Abs 2 KI-VO)**

Die Kommission schlägt die Streichung der Registrierungspflicht nach Art 49 Abs 2 KI-VO vor. Nach Art 49 Abs 2 KI-VO sind Anbieter:innen einer Hochrisiko-KI-Systems, die zu dem Schluss gelangen, dass dieses nach Art 6 Abs 3 KI-VO nicht hochriskant ist, zur Registrierung dieses Systems in einer in Art 71 KI-VO genannten EU-Datenbank verpflichtet, bevor das KI-System in Verkehr gebracht oder in Betrieb genommen wird. Die Registrierungspflicht in Art 49 Abs 2 KI-VO wurde als Schutzmaßnahme eingeführt, um Transparenz und öffentliche Rechenschaftspflicht für Unternehmen sicherzustellen, die das von ihnen entwickelte KI-System von der Hochrisiko-Klassifizierung ausnehmen wollen. Der Registrierungsprozess ist bürokratisch minimal aufwendig, aber aus Sicht von Betroffenen höchst relevant. Denn die von einem Anbieter erteilten Informationen ermöglichen eine externe Überprüfung von Ausnahmeentscheidungen.

Der Vorschlag, diese Registrierungsverpflichtungen zu streichen, ist deshalb aus Sicht der AK abzulehnen. Anbieter:innen würden die Möglichkeit behalten, sich durch Selbstbewertung der Hochrisiko-Klassifizierung zu entziehen, ohne dass diese Entscheidungen öffentlich dokumentiert oder einer Aufsicht unterworfen sind. Dies schafft eine Lücke in der KI-VO, die besonders bedenklich ist, da KI-Systeme nach Art 6 Abs 3 KI-VO per Definition zunächst die Kriterien für eine Hochrisikoklassifizierung aufgrund ihres beabsichtigten Zwecks und Anwendungskontexts erfüllen.

Außerdem kann die Streichung der Pflicht zur Registrierung dazu führen– wie schon jetzt der Umgang mit der DSFA (Art 35 DSGVO) zeigt –, dass die Ausnahme in Art 6 Abs 3 KI-VO von vielen Organisationen willkürlich weit ausgelegt wird, oder dass die Dokumentation de facto nicht gemacht wird. Damit haben jene Organisationen, die rechtskonform und gewissenhaft arbeiten, sowie die von einem solchen System betroffenen Personen den Nachteil.

- **Art 43 Abs 3 KI-VO – Konformitätsbewertung**

Art 43 KI-VO behandelt die Konformitätsbewertung von Hochrisiko-KI-Systemen, wobei dessen Absatz 3 die unter Anhang I Abschnitt A fallenden Hochrisiko-KI-Systeme regelt. Danach haben die Anbieter:innen die in den aufgelisteten Vorschriften festgelegten Anforderungen zu erfüllen, wobei die für sie relevanten Anforderungen der KI-VO in die Bewertung miteinbezogen werden müssen. Die gemäß diesen aufgelisteten Rechtsakten notifizierte Stelle ist zu dieser Bewertung berechtigt, wobei sie nach dem Vorschlag der Kommission in Art 43 Abs 3, 2. Unterabsatz des Entwurfs zur KI-VO die Ernennung als hierfür zuständige Stelle spätestens 18 Monate nach Anwendbarkeit der KI-VO beantragen muss.

Fällt ein Hochrisiko-KI-System sowohl unter eine unionsrechtliche Harmonisierungsvorschrift von Abschnitt A des Anhang I als auch unter eine der Kategorien des Anhangs III, so haben Anbieter:innen das in den spezifischen Unionsvorschriften relevante Bewertungsverfahren einzuhalten (Art 43 Abs 3 letzter Unterabsatz des Vorschlags zur KI-VO).

Unklar ist zunächst, weshalb sich die bereits für die Konformitätsbewertung nach den spezifischen unionsrechtlichen Harmonisierungsvorschriften zuständigen Stellen nunmehr auch als nach der KI-VO zuständige Stelle zu bewerben haben und was im Falle des Unterbleibens dieser Beantragung geschieht. Unbeantwortet bleibt auch, was in der Zeit zwischen Anwendbarkeit der KI-VO (i.e. 2. August 2026 nach Art 113 KI-VO) und Beantragung als nach der KI-VO zuständige Stelle passiert. Auch der hier relevante Erwägungsgrund 8 des Vorschlags der Kommission schafft keine diesbezügliche Klarheit. Die AK regt daher an, die angeführten offenen Punkte zB in einem Erwägungsgrund zu erläutern.

- **Art 50 Abs 7 KI-VO – Transparenzpflichten für Anbierter:innen und Betreiber:innen bestimmter KI-Systeme; Streichung der Durchführungsrechtsakte**

Nach Art 50 Abs 7 KI-VO soll die Ausarbeitung von Praxisleitfäden für die wirksame Umsetzung der Pflichten bezüglich Feststellung und Kennzeichnung künstlich erzeugter oder manipulierter Inhalte durch das Büro für Künstliche Intelligenz gefördert und erleichtert werden. Die Kommission kann zur Genehmigung dieser Praxisleitfäden Durchführungsrechtsakte erlassen, womit dem Praxisleitfaden allgemeine Gültigkeit verliehen wird.

Diese Möglichkeit der Durchführungsrechtsakte durch die Kommission zur Genehmigung dieser Praxisleitfäden soll laut Vorschlag nun gestrichen werden. Aus Verbraucher:innensicht ist dies jedenfalls abzulehnen und dient keineswegs der Rechtssicherheit. Ohne Durchführungsrechtsakte bleibt es bei freiwilligen Leitfäden ohne rechtlich durchsetzbare Konsequenzen im Falle der Nichteinhaltung, was jedenfalls abzulehnen ist.

- **Art 57 Abs 3a Schaffung eines KI-Reallabors auf EU-Ebene für KI-Systeme nach Art 75 Abs 1**

Der Vorschlag wird ausdrücklich begrüßt, insbesondere da damit die Notwendigkeit spezieller Rechtsgrundlagen für KI-Training in der DSGVO (Änderungsvorschläge für Art 9 Abs 2 DSGVO bzw Art 88c DSGVO) entfällt. Unter Aufsicht der zuständigen Behörde können bereits jetzt Hochrisiko-KI-Systeme bzw. mit Schaffung dieses zusätzlichen Reallabors auch dem Art 75 KI-VO unterliegende KI-Systeme trainiert werden, ohne den Datenschutz generell einschränken zu müssen.

- **Art 60a des Entwurfs zur KI-VO – Tests von in Abschnitt B des Anhangs I aufgelisteten Hochrisiko-KI-Systemen unter Realbedingungen außerhalb von KI-Reallaboren**

Art 60a des Entwurfs zur KI-VO soll für in Abschnitt B des Anhangs I aufgelistete Produkte eine – im Vergleich zu Art 60 KI-VO – erleichterte Testung unter Realbedingungen ermöglichen. Betroffen sind hievon KI-Systeme im Zusammenhang mit Fortbewegungsmitteln wie etwa Kraftfahrzeugen, Eisenbahnfahrzeugen oder Schiffsausrüstungen.

Aus Sicht der AK ist die Notwendigkeit einer derart erleichterten Testung unter Realbedingungen für diese Gruppe von KI-Systemen zu hinterfragen. Es sollte besser wie bisher Art 60 KI-VO angewandt werden, womit sichergestellt ist, dass sämtliche damit normierten Schutzmaßnahmen einzuhalten sind.

- **Art 72 des Entwurfs zur KI-VO – Beobachtung nach dem Inverkehrbringen durch Anbieter:innen und Plan für die Beobachtung nach dem Inverkehrbringen für Hochrisiko-KI-Systeme**

Nach Art 72 KI-VO haben Anbieter:innen nach dem Inverkehrbringen des Hochrisiko-KI-Systems ein System zur Beobachtung einzurichten und zu dokumentieren. Art 72 Abs 3 KI-VO, der einen Plan für die Beobachtung nach dem Inverkehrbringen vorschreibt, soll nach dem Vorschlag der Kommission nun dahingehend geändert werden, dass die Kommission bloß noch Leitlinien für einen derartigen Plan für die Beobachtung nach dem Inverkehrbringen zu erarbeiten hat und nicht mehr wie derzeit einen diesbezüglichen Durchführungsrechtsakt zu erlassen hat.

Die AK spricht sich gegen bloße Leitlinien aus; die derzeitige Bestimmung des Art 72 Abs 3 KI-VO sollte besser unverändert bestehen bleiben, womit verbindliche Rechtsakte (anstelle von freiwilligen Leitlinien) sichergestellt sind.

- **Art 75 des Entwurfs zur KI-VO – Amtshilfe, Marktüberwachung und Kontrolle von KI-Systemen mit allgemeinem Verwendungszweck**

Art 75 KI-VO soll nach dem Vorschlag zunächst eine neue Überschrift erhalten: „Market surveillance and control of AI systems and mutual assistance" statt bisher wie oberhalb angeführt.

Neben der Überschrift wird aber auch die Bestimmung des Art 75 Abs 1 geändert und um die Absätze 1a bis 1c ergänzt. Nach dem vorgeschlagenen Art 75 Abs 1 KI-VO soll das Büro für Künstliche Intelligenz auch für die Überwachung und Durchsetzung der Verpflichtungen dieser Verordnung in Zusammenhang mit KI-Systemen, die in einer designierten sehr großen Online-Plattform oder sehr großen Online-Suchmaschine im Sinne des DSA zuständig sein. Dies ist stimmig, zumal der EK auch Kompetenzen bezüglich VLOPs und VLOSEs nach dem Digital Services Act (DSA) zukommen.

Die weiteren vorgeschlagenen Absätze 1a bis 1c beinhalten Durchführungsrechtsakte für die Ausgestaltung der diesbezüglichen Kompetenzen des Büros für Künstliche Intelligenz (Abs 1a), einen Verweis auf die Marktüberwachungsverordnung (Abs 1b) und eine Pflicht der Kommission zur Konformitätsbewertung bei Hochrisiko-KI-Systemen vor dem Inverkehrbringen, wobei diese Bewertung auch an notifizierte Stellen ausgelagert werden kann (Abs 1c).

Die Änderungen werden aus Sicht der AK begrüßt, da damit die Kontrolle insbesondere über große KI-Systeme bzw. KI-Modell-Anbieter gestärkt wird.

- **Art 77 des Entwurfs zur KI-VO – Befugnisse der für den Schutz der Grundrechte zuständigen Behörden**

Zunächst schlägt die Kommission eine Änderung der Überschrift vor, womit auch die Kooperation mit den

Marktüberwachungsbehörden in der Überschrift angeführt wird.

Darüber hinaus wird der Anwendungsbereich der nationalen Behörden und Stellen nun nicht mehr auf Hochrisiko-KI-Systeme nach dem Anhang III beschränkt. Der Wegfall dieses Verweises auf Anhang III wird begrüßt, da damit bspw. auch die Maschinen-VO (die für die Sicherheit und Gesundheit der Arbeitnehmer:innen relevant ist) erfasst wird. Auch das Hinzufügen von Informationen (neben wie bisher Dokumentationen), zu denen nun Zugang zu erteilen ist, ist aus Sicht der AK zu begrüßen.

Die Einholung der Informationen und Dokumentation nach dem Vorschlag über die zuständige Marktüberwachungsbehörde wird voraussichtlich eine Erleichterung der Ausübung der Aufgaben der Art 77-Stellen bringen, da damit eine zentrale Stelle mit der Besorgung der Dokumentation betraut wird (dh dass die Dokumentation nicht über einzelne Arbeitgeber angefragt werden muss) und die Kooperation zwischen Art 77-Stellen und der zuständigen Marktüberwachungsbehörde erleichtert wird.

- **Art 111 des Entwurfs zur KI-VO – Bereits in Verkehr gebrachte oder in Betrieb genommene KI-Systeme und bereits in Verkehr gebrachte KI-Modelle mit allgemeinem Verwendungszweck**

- **Art 113 KI-VO – Inkrafttreten und Geltungsbeginn**

Nach dem Vorschlag der Kommission soll Art 111 Abs 2 KI-VO geändert werden und ein neuer Absatz 4 angefügt werden.

Art 111 Abs 2 KI-VO regelt die Anwendung der KI-VO für Betreiber:innen von Hochrisiko-KI-Systemen, die bereits vor dem 2.8.2026 in Verkehr gebracht oder in Betrieb genommen wurden. Nach dem Vorschlag der EK wird hier nun nicht mehr ein konkretes Datum (2. August 2026) genannt, sondern auf das Datum der Anwendbarkeit des Kapitels III und der korrespondierenden Verpflichtungen nach Art 113 verwiesen.

Art 111 KI-VO soll nach dem Vorschlag um einen neuen Absatz 4 ergänzt werden, wonach Anbieter von KI-Systemen inklusive solcher mit allgemeinem Verwendungszweck, die synthetische Audio-, Bilder, Video- der Textinhalte generieren, die vor dem 2. August 2026 auf den Markt gebracht werden, den Anforderungen des Art 50 Abs 2 mit 2. Februar 2027 zu entsprechen haben.

Akteur:innen und Betreiber:innen solcher KI-Systeme sind hievon jedoch nicht umfasst und haben diese Bestimmung daher bereits mit 2. August 2026 einzuhalten. Eine derartige Unterscheidung entbehrt jeglicher Rechtfertigung, weshalb dieser zusätzliche Absatz ersatzlos gestrichen werden sollte.

Art 113 KI-VO soll nach dem Entwurf dergestalt geändert werden, dass Kapitel III, Abschnitte 1, 2 und 3 nach einer Entscheidung der Kommission, dass adäquate Maßnahmen zur Unterstützung der Einhaltung der Bestimmungen des Kapitel III verfügbar sind, 6 Monate nach dieser Entscheidung in Bezug auf Hochrisiko-KI-Systeme nach Art 6 Abs 2 und Anhang III bzw. nach 12 Monaten in Bezug auf Hochrisiko-KI-Systeme nach Art 6 Abs 1 und nach Anhang I bzw. bei Fehlen einer solchen Entscheidung ab 2. Dezember 2027 bzw. ab 2. August 2028 gelten.

Damit wird der Geltungsbeginn vom 2. August 2026 auf den 2. Dezember 2027 bzw. den 2. August 2028 hinausgeschoben, was von der AK jedenfalls abgelehnt wird. Die Verschiebung bringt weitere Rechtsunsicherheit und wird daher entschieden abgelehnt.

Unklar ist nach Durchsicht dieses Vorschlags auch, ab wann nun Art 6 Abs 1 KI-VO zu gelten hat. In Art 113 lit c KI-VO, der nach dem Entwurf nicht geändert werden soll, wird der Geltungsbeginn von Art 6 Abs 1 mit 2. August 2027 festgelegt. Nach der nun neu vorgeschlagenen lit d 2. Unterabsatz (ii) des Art 113 soll der Geltungsbeginn spätestens mit 2. August 2028 festgesetzt werden, was aus Sicht der AK wie oben ausgeführt, abzulehnen ist.

Kontaktieren Sie uns!

In Wien:

Jasmin Reininger
T +43 (1) 501 65 12801
jasmin.reininger@akwien.at

Louise Beltzung
T +43 (1) 501 65 12324
louise.beltzung@akwien.at

Jakob Kalina
T +43 (1) 501 65 13720
jakob.kalina@akwien.at

In Brüssel:

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

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

www.arbeiterkammer.at

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 Arbeitnehmer:innen und Konsument:innen 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.