23.01.2026

Anhang zum Positionspapier: Stellungnahme zu den Einzelregelungen im Digital-Omnibus-Paket

Die Europäische Kommission hat am 19. November 2025 ihr siebtes Omnibus-Paket vorgestellt und holt dazu Stellungnahmen bis zum 11. März 2026 ein. Dieses Positionspapier nimmt zu den enthaltenen Verordnungsvorschlägen für einen „Digital Omnibus“ zu Daten, einen „Digital Omnibus on AI“ Stellung und einen Verordnungsvorschlag über European Business Wallets Stellung.[1] Die Verordnungsvorschläge liegen bisher nur auf Englisch vor.

a) Digital Omnibus (Daten): Änderungen des Data Act

Vorschrift	Inhalt	Stellungnahme
---	Zusammenfassung von FFDR, DGA, Data Act, Offene-Daten-RL im Data Act	**Zusammenfassung grundsätzlich sinnvoll**, da Systematik zurzeit unklar und Überschneidungen zwischen Rechtsakten. Umwandlung der Offene-Daten-RL in **Verordnungsrecht** aber nicht unproblematisch: Die Kontrolle über Informationen des öffentlichen Sektors, um deren Verfügbarkeit und Weiterverwendung es nach der Richtlinie geht (Erw.-Grd. 16), kann für **innere und äußere Sicherheit der Mitgliedstaaten relevant** sein. **Alternativ** zur Zusammenfassung der Regelungen zur Datenweiterverwendung im Data Act könnten die **DGA-Regelungen** hierzu auch **in die Offene-Daten-Richtlinie integriert** und den Mitgliedstaaten Umsetzungsspielräume belassen werden.
---	Vorratsdatenspeicherung wird getrennt geregelt	Sinnvoll, da **eigenständige Problematik:** Zugriff auf personenbezogene Daten zu Sicherheitszwecken.
Art. 1 Abs. 2(d)	Übernahme der DGA-Regelungen zu Datenvermittlungsdiensten/Datenaltruismus in Data Act	Die Regelungen haben sich **nicht bewährt** und sollten besser ersatzlos wegfallen. Eine spätere Evaluation (Art. 1 Abs. 26 = Art. 49 Data Act n.F.) bietet keinen erkennbaren Mehrwert.

[1] COM(2025) 836 final bzw. COM(2025) 837 final.

Vorschrift	Inhalt	Stellungnahme
Art. 1 Abs. 2(e)	Definition 'medium-sized enterprise'/'small mid-cap'	**Mehrere Kategorien von Kleinunternehmen**, für die Sonderregelungen gelten, **vermindern** die **Rechtsklarheit**. Sie indizieren auch, dass die Regeln des Digital-Omnibus die Wirtschaft weiter übermäßig belasten.
Art. 1 Abs. 3, 4	Einführung eines Weigerungsrechts von Geschäftsgeheimnisinhabern beim Datenzugang (Art. 4 Abs. 8, Art. 5 Abs. 11 Data Act)	Die Verpflichtung von Datenempfängern, die **Geschäftsgeheimnisse** des urspr. Dateninhabers zu schützen, führt zu **schwer zu überblickenden Risiken** für den Dateninhaber. Die Vereinbarung zwischen Produktnutzer und Empfänger stellt insoweit einen Vertrag zulasten Dritter (urspr. Dateninhaber) dar. **Rechtsunsicherheit** durch Kombination **stark wertungsbedürftiger Rechtsbegriffe** („exceptional circumstances", „highly likely" „serious economic damage", „on a case-by-case basis"). Der **Datenzugang** sollte nach Data Act **wie nach EDHS-VO** ausgestaltet werden. Der Regulierungsansatz des Data Act ist insgesamt verfehlt.
Art.1 Abs. 6-14	Begrenzung des Datenzugangs für öffentliche Stellen auf Fälle „öffentlicher Notlagen" anstelle von „außergewöhnlicher Notwendigkeit"	Die Begrenzung **reduziert den** potenziellen **Aufwand** für Unternehmen und erscheint mit Blick auf das Ziel der Wettbewerbsfähigkeit **unproblematisch**.
Art. 1 Abs. 15	Regelungen zu Cloud-Wechsel (Art. 23 ff. Data Act) werden vereinfacht (neuer Art. 31 Abs. 1a, 1b Data Act).	**Regulierungsansatz zu hinterfragen:** Neben Speichern werden sehr spezifische Dienste nachgefragt → Bedarf für die Wechselregelungen in Art. 23 ff. Data Act ist insgesamt unklar. Wechsel wird weniger durch inkompatiblen Funktionsumfang, eher durch inkompatible Softwarearchitekturen/Schnittstellen und Datenformate erschwert.
At. 1 Abs. 16	Wiederverwendung öffentlicher Daten unter Vorbehalt, dass Zugriff von Drittstaaten verhindert werden kann (Art. 32 Data Act)	Sinnvoll zur **Stärkung von Resilienz im EU-Außenverhältnis.** **Ausgestaltung der Regelung aber unklar:** Verweisungen auf sonstige Regelungen, wertungsbedürftige Rechtsbegriffe („minimum amount of data permissible"; „reasonable interpretation")

Vorschrift	Inhalt	Stellungnahme
Art. 1 Abs. 17	Streichung der Regelung über intelligente Verträge (Art. 36 Data Act)	Sinnvoll, die Regelung ist unpraktikabel und führt zu Rechtsunsicherheit (so die EU-Kommission selber; COM(2025) 837 final, S. 5 und Erw.-Grd. 16).
Art. 1 Abs. 18	Übernahme von DGA-Regelungen zu Datenvermittlungsdiensten und Daten-Altruismus	Die **Regelungen** haben sich **nicht bewährt** und sollten anstelle der vorgesehenen Straffung innerhalb des Data Act (Art. 32a ff. n.F.) besser ersatzlos wegfallen. Eine spätere Evaluation (Art. 1 Abs. 26 = Art. 49 Data Act n.F.) bietet keinen erkennbaren Mehrwert.
Art. 1 Abs. 18	Übernahme von DGA-Regelungen zur Wiederverwendung öffentlicher Daten	Die **Übernahme dieser Regelungen (Art. 32i ff. Data Act n.F.) ist sinnvoll**. Dadurch werden für öffentliche Daten einheitliche Standards geschaffen. Die **Zusammenführung mit den Regelungen der Offene Daten-Richtlinie (Art. 32n ff. Data Act n.F.)** ist zwar ebenfalls sinnvoll, wegen der Bedeutung der betroffenen Daten für die souveräne Informationsverwaltung der Mitgliedstaaten aber nicht unproblematisch (s.o. Zeile 1). Insbesondere die Regelungen über die **Identifizierung „hochwertiger Datensätze“** (Art. 14 RL (EU) 2019/1024; Art. 32v Data Act n.F.) enthalten zudem viele wertungsbedürftige Rechtsbegriffe. Sie tragen dadurch **kaum** zur **Rechtssicherheit** bei. Besser wäre ohnehin eine umfassende Vereinheitlichung der Regeln für öffentliche Daten, soweit diese statistisch oder wissenschaftlich nutzbar sind: • Der Datenzugang ist bislang zersplittert geregelt (s.a. RL 2007/2/EG; RL 2003/4/EG); • Doppelungen in Sonderregimes wie z. B. für Gesundheitsdaten (VO 2025/327 – EDHS) sollten für mehr Rechtsklarheit reduziert werden (z. B. zu Rechten/Dokumentation/Complianceanforderungen).
Art. 1 Abs. 18	Übernahme des Datenlokalisierungsverbots der FFDR in den Data Act	Die Übernahme des **Datenlokalisierungsverbots (Art. 32h Data Act n.F.) ist vertretbar**, aber die praktische Bedeutung wohl begrenzt. Der Wegfall der FFDR-Vorschriften zu Verhaltenskodizes über Datenteilung ist wegen der begrenzten Regelungswirkung vertretbar.

Vorschrift	Inhalt	Stellungnahme
		Im Interesse an einer allgemeinen **Förderung von Interoperabilität und einheitlichen Datenformaten** sollte dann jedoch der **Anwendungsbereich der Art. 33 ff. Data Act über Europäische Datenräume hinaus erweitert** werden.

b) Digital Omnibus (Daten): Änderungen von Datenschutz-Grundverordnung und ePrivacy-Richtlinie

Im Vorgriff auf die Vorstellung des Digital Omnibus hatte Deutschland der Europäischen Kommission Vorschläge für eine Vereinfachung der DSGVO übermittelt. Dieses **„German proposal for simplification of the GDPR“** wurde von Netzpolitik.org vom 23. Oktober 2025 veröffentlicht und ist nach der Folgenabschätzung zum Digital-Omnibus-Paket in dieses eingeflossen. Deshalb wird es in der folgenden Stellungnahme ebenfalls berücksichtigt.

DSGVO

Vorschrift	Inhalt	Deutsche Position	Stellungnahme
---	Zusammenfassung von DSGVO und e-Privacy-RL 2002/58/EG.	---	Grds. sinnvoll.
---	---	Forderung des besseren Ausgleichs zwischen betroffenen Schutzgütern: • Allg. Persönlichkeitsrecht der Betroffenen einer Datenverarbeitung • Wirtsch. Freiheit/Wissenschafts-Freiheit der Datenverarbeiter	Zusätzlich beachten: • Öffentliches Interesse an Datennutzung bei Erfüllung behördlicher Aufgaben • Digitale Souveränität (Resilienz) gegenüber Nicht-EU-Staaten; aber auch Grenzen f. EU-Industriepolitik (Art. 173 AEUV)

Vorschrift	Inhalt	Deutsche Position	Stellungnahme
Art. 3 Abs. 1	Neufassung der Definition von „personenbezogenen Daten“ (Art. 4 DSGVO):	---	Einführung eines „subjektiven Ansatzes“, der den Geltungsbereich des Gesetzes auf Situationen beschränkt, in denen eine Person von einem bestimmten Unternehmen identifiziert werden kann. Die Neuregelung setzt EuGH C-413/23 P – *EDSB* um. Sie geht aber mit dem Risiko einher, dass **Unternehmen strategisch** zwar für sich selbst ausschließen, dass sie personenbezogene **Daten sammeln**, aber dass sie zugleich sicherstellen, dass Sie ihren Geschäftspartnern Daten zur Verfügung stellen, die dort personenbezogen sein können (ohne dass die Betroffenen mit diesen anderen Unternehmen eine direkte Beziehung haben). Außerdem wird die Beurteilung der Datensammlung nach DSGVO durch stark wertungsbedürftige Begriffe erschwert („not [...] personal [...] where that entity cannot identify the natural person [...] taking into account the means reasonably likely to be used by that entity.“). Insoweit dürfte die Neuregelung **erhebliche Beweisschwierigkeiten** in Streitfällen mit sich bringen. **Besser** wäre es, den **Anwendungsbereich der DSGVO insgesamt genauer an den relevanten Grundrechtsfragen auszurichten** und insbesondere zwischen staatlicher und unternehmerischer Datenverarbeitung zu differenzieren.
---	---	Prüfung eines **3-Layer-Model** (s. z. B. Wendehorst): Umfangreiche Pflichten für Großunternehmen, reguläre Pflichten, verminderte Pflichten/Ausnahmen für KMU	**Abzulehnen: Die Schutzbedürftigkeit Betroffener hängt nicht von der Größe des verarbeitenden Unternehmens, sondern von den Risiken der Verarbeitung ab** („same risk – same regulation“). Datenschutzvorgaben müssen sich zudem auf das Erforderliche beschränken, um mit der unternehmerischen Freiheit (Art. 16 GRCh) vereinbar zu sein. Die erforderlichen Vorgaben können von großen Unternehmen sogar i.d.R. besser umgesetzt werden als von kleineren. Großunternehmen haben hierfür mehr Ressourcen.

Vorschrift	Inhalt	Deutsche Position	Stellungnahme
		und nicht-wirtschaftliche Tätigkeiten prüfen	**Besser** wäre es, den **Anwendungsbereich der DSGVO insgesamt genauer an den relevanten Grundrechtsfragen auszurichten** und insbesondere zwischen staatlicher und unternehmerischer Datenverarbeitung zu differenzieren.
Art. 3 Abs. 2	Rückkopplung des Zweckbindungsgrundsatzes (Art. 5 Abs. 1 lit. b DSGVO) an die Zweckbegrenzungsregelung in Art. 6 Abs. 4 DSGVO	---	Sinnvolle Klarstellung.
Erw.-Grd. 30 f.	Datennutzung für KI-Training sollte als „berechtigtes Interesse“ anerkannt werden.	Safe Harbor, um KI-Systeme DSGVO-konform aufzusetzen.	**Der Digital Omnibus verzichtet auf eine Änderung des Gesetzestextes (Art. 6 Abs. 1 lit. f DSGVO). Die Regelung reicht damit nicht aus zur Schaffung von Rechtssicherheit.** Hierfür wären im Übrigen auch Regelungen für die Nutzung von urheberrechtlich geschützten Inhalten und Geschäftsgeheimnissen für das Training von KI-Modellen erforderlich.
Art. 3 Abs. 3	Einschränkung des Schutzes für bes. geschützte Daten (Art. 9 DSGVO) für Fälle des Trainings von KI-Modellen und für Verarbeitung biometrischer Daten zur Identitätsprüfung	Zugriff auf bes. geschützte Daten (Art. 9 DSGVO) sollte (nur) in Notsituationen (z. B. Pandemie) vereinfacht werden.	Die **Freistellung** der Nutzung besonders geschützter Daten **für Zwecke des KI-Trainings** dient dem Schutz unternehmerischer Freiheit (Art. 16 GRCh) bei der Entwicklung innovativer KI-Produkte, aber **schränkt den Grundrechtsschutz für Betroffene empfindlich ein.** Die **Vorgabe**, dass geeignete („appropriate“) **technische und organisatorische Maßnahmen** getroffen werden müssen, um die Sammlung relevanter Daten zu minimieren und solche Daten zu schützen (Art. 9 Abs. 5 DSGVO n.F.), **reicht nicht aus.** Zusätzlich müsste die Rechtsposition der Betroffenen gestärkt werden, z. B. durch eine Vermutungsregelung in Bezug auf Schäden. Die Vereinbarkeit mit Art. 7, 8 GRCh ist daher zweifelhaft.

Vorschrift	Inhalt	Deutsche Position	Stellungnahme
			Der Unionsgesetzgeber wird mit der Regelung davon abgesehen seiner **Schutzpflicht mit Blick auf Ausbeutungsrisiken** zum Nachteil von Verbrauchern nicht gerecht. Die **Nutzung biometrischer Daten** soll auf Fälle beschränkt sein, in denen die Daten unter **alleiniger Kontrolle des Grundrechtsbetroffenen** stehen. Die Regelung erscheint vertretbar. Der **deutsche Vorschlag ist sinnvoll.**
Art. 3 Abs. 4	Einschränkung der kostenfreien Information über die Datenerhebung bei der betroffenen Person oder anderweitig (Art. 12 Abs. 5 DSGVO).	Beschränkung missbräuchlicher Auskunftsanfragen (Art. 15, 57 DSGVO).	Die Regelung des **Digital Omnibus** schränkt das Recht auf kostenfreie Information für missbräuchliche Auskunftsanfragen ein, wobei die Beweislast für einen Missbrauch beim Datenverarbeiter liegt. Die **Regelung erscheint vertretbar.** Die deutschen Vorschläge sind dagegen zu schwerfällig.
Art. 3 Abs. 5	Begrenzung der Information über die Datenerhebung bei der betroffenen Person (Art. 13 Abs. 4 DSGVO) im Rahmen bestehender Rechtsverhältnisse und bei schon vorhandener Information beim Betroffenen.	Verminderung von Informationspflichten (Art. 13 DSGVO): Unternehmen sollten relevante Informationen nur auf eigener Website vorhalten.	Die **Regelung des Digital Omnibus** schränkt das Recht auf Information in Fällen ein, in denen der Betroffene die Informationen zur Wahrnehmung seiner Rechte nicht benötigt. Die Regelung enthält viele wertungsbedürftige Rechtsbegriffe („clear and circumscribed relationship"; "activity that is not data-intensive"; "reasonable grounds") und erscheint damit **kaum praktikabel.** Besser wäre es, die Betroffenen schlichtweg an den Kosten der Informationsbereitstellung zu beteiligen. **Der deutsche Vorschlag ist problematisch wegen Manipulationsrisiken.** Wenn überhaupt, sollten relevante Informationen auf vertrauenswürdigen Drittseiten vorgehalten werden. Die **Ausnahmen** (Weitergabe an Dritte; besondere Schutzbedürftigkeit) **zeichnen grundrechtliche Grenzen nach.** Diese Ausnahmen dürften also grundsätzlich zwingend sein.

Vorschrift	Inhalt	Deutsche Position	Stellungnahme
Art. 3 Abs. 6	Einschränkung der kostenfreien Information über die Datenerhebung zu wiss. Zwecken	---	Die Regelung **schränkt die Möglichkeiten zur Datennutzung zu wissenschaftlichen Zwecken ein.** Sie enthält viele wertungsbedürftige Rechtsbegriffe („disproportionate effort"; „seriously impair"; „appropriate measures") und erscheint damit **kaum praktikabel.**. Besser wäre es, die Antragsteller schlichtweg an den Kosten der Informationsbereitstellung zu beteiligen.
Art. 3 Abs. 7	Begrenzung des Rechts, kein Gegenstand automatischer Datenverarbeitung (inkl. Profiling) zu sein (Art. 22 Abs. 1 DSGVO)	---	Die **Regelung beschränkt den Rechtsschutz.** Die trägt allerdings dem Umstand Rechnung, dass das Recht in der Praxis ohnehin nur auf dem Papier besteht. Sie erscheint **vertretbar.**
Art. 3 Abs. 8	Verlängerung der Fristen für die Meldung von Verletzungen; einheitliche Meldestelle und Übergangsregime; Formulare (Art. 33 DSGVO).	Nötige Vereinfachung der Meldung von Verletzungen; Ersetzung der 72-Stunden-Frist durch Frist v. 3 Arbeitstagen (Art. 33 DSGVO).	Die Regelungen des **Digital Omnibus erleichtern den Rechtsschutz** für Betroffene und **reduzieren tendenziell den behördlichen Aufwand.** Sie erscheinen daher sinnvoll.
Art. 3 Abs. 9	Präzisierung der Notwendigkeit und Anforderungen an Datenschutz-Folgenabschätzungen (Art. 35 DSGVO)	---	Die Regelung sieht Vereinheitlichungen vor („common template"), aber verwendet wertungsbedürftige Begriffe hinsichtlich der festzulegenden Anforderungen. Im Interesse der Rechtsklarheit wäre es sinnvoll, wenn zumindest die **Branchen definiert** würden, in denen **Datenschutz-Folgenabschätzungen vorzunehmen** sind.
Art. 3 Abs. 10	Ermächtigung der EU-Kommission zu delegierter Rechtsetzung in Bezug auf Pseudonymisierung	Klarstellung: Anonymisierte Daten sind keine personenbezogenen Daten – aber: Anonymisierung ist Verarbeitung schutzwürdiger Daten.	Die Regelung im Digital Omnibus kann keine Rechtssicherheit schaffen: Der **Wegfall des Personenbezugs ist Tatsachenfrage. Die Regelung ist abzulehnen.** Der **deutsche Vorschlag** ist **dagegen zur Klarstellung des Begriffs „Datenverarbeitung" sinnvoll.**

Vorschrift	Inhalt	Deutsche Position	Stellungnahme
---	---	In Art. 42 ff. DSGVO ist mehr Raum für Zertifizierungen zu geben; insb. durch Möglichkeit einer Hersteller-/Lieferantenzertifizierung, statt allein Verarbeiter haften zu lassen.	Der Digital Omnibus hat den **deutschen Vorschlag** nicht aufgegriffen. Der Vorschlag erscheint dennoch **sinnvoll.**
	---	Zusätzliche Regelungen zum Jugend-/Verbraucherschutz.	Die deutschen Vorschläge wurden im Digital Omnibus nicht aufgegriffen, erscheinen aber sinnvoll.
	---	Leitlinien für Datenschutz bei Archivierung.	
	---	Erleichterung der Datennutzung für F&E, wenn konkreter Nutzungszweck bei Datensammlung noch unbekannt.	

c) DSGVO und ePrivacy-RL (RL 2002/58/EG)

Vorschrift	Inhalt	Stellungnahme
Art. 3 Abs. 15; Art. 5 Abs. 2	Einschränkung der Platzierung von Cookies u.ä. auf den Nutzer-Endgeräten; insofern Neuregelung in Art. 88a, 88b DSGVO ausgehend vom bisherigen Art. 5 Abs. 3 RL 2002/58/EG.	Der Umstand, dass der **Digital Omnibus** nicht lediglich einen Opt-out für Tracking Cookies vorsieht, wie es zuvor in der Presse kolportiert wurde, ist zu begrüßen. **Tracking Cookies sind AGB- und datenschutzrechtlich problematisch.** Die Nutzung sollte auf Dauer zugunsten datenschutzfreundlicherer Technologien wie z. B. einer Entscheidungsmaske im Webbrowser (vgl. Art. 88b Abs. 6 DSGVO)

Vorschrift	Inhalt	Stellungnahme
		eingeschränkt werden. Dabei ist jedoch zu berücksichtigen, dass die zentrale Steuerung von Einwilligungen z. B. über einen Webbrowser **schwer zu implementieren** ist, weil Einwilligungen zweckgebunden erteilt werden. Die vorgeschlagenen Regelungen sollten deshalb überprüft werden, um einen fairen Ausgleich der Interessen von Vermittlungsdiensten, der Werbewirtschaft und der Verbraucher als Grundrechtsträger zu erreichen. Davon abgesehen sollte geprüft werden, **RL 2002/58/EG** zur Rechtsklarheit **insgesamt in die DSGVO zu integrieren.**
Art. 5 Abs. 1	Streichung von Art. 4 RL 2002/58/EG	Die zu streichende Vorschrift macht Vorgaben zur Sicherheit der Datenverarbeitung, dürfte aber durch Art. 25 DSGVO und RL 2022/2555 (NIS 2) überholt sein.

d) Digital Omnibus (Daten): Änderungen der NIS 2-Richtlinie

Vorschrift	Inhalt	Stellungnahme
Art. 6-9	Einheitliche Meldestelle für IT-Sicherheitsvorfälle (NIS2-RL, eIDAS-VO, Critical Entities-VO, DORA; DSGVO)	Die Regelungen des **Digital Omnibus erleichtern den Rechtsschutz** für Betroffene und **reduzieren tendenziell den behördlichen Aufwand.** Sie erscheinen daher sinnvoll.

e) Digital Omnibus on AI: Änderungen der KI-Verordnung

Vorschrift	Inhalt	Stellungnahme
---	Der Digital Omnibus on AI soll Umsetzungsschwierigkeiten ausräumen, die den effektiven Anwendungsbeginn der Hauptvorgaben der KI-VO gefährden könnten (COM(2025) 836 final, S. 2)	**Änderungen der KI-VO reichen nicht aus zur Schaffung von Rechtssicherheit und zur Verminderung bürokratischer Lasten.** Dafür wäre es insbesondere auch nötig, die Pflichten-/Haftungsverdoppelungen durch KI-VO einerseits und DSGVO/AVMD/DSA/RL über unlautere Geschäftspraktiken usw. andererseits zu beseitigen. Außerdem werden die **relevanten Risiken** nach der gegenwärtigen KI-VO **fast alle**

Vorschrift	Inhalt	Stellungnahme
		als potenziell systemisch angesehen (Ausn.: Art. 51 ff.). Hier wäre zu differenzieren, um der Marktbedeutung des jeweiligen Einsatzes stärker Rechnung zu tragen.
---	Ankündigung von 13 weiteren Leitlinien zur Konkretisierung der KI-VO und zur Erleichterung ihrer Anwendung	**Eine Vielzahl ergänzender Leitlinien trägt nicht zur Rechtssicherheit und Anwendungserleichterung bei.** Die Notwendigkeit solcher Leitlinien indiziert einen missglückten Regelungsansatz der KI-VO. Die Leitlinien erhöhen den Umsetzungsaufwand zudem in einem Maße, das überhaupt nur durch größere Unternehmen zu bewältigen sein dürfte.
Art. 1 Abs. 1, 3	Erweiterung der Privilegierung von Kleinunternehmen (SMC neben SME).	**Mehrere Kategorien von Kleinunternehmen**, für die Sonderregelungen gelten, **vermindern** die **Rechtsklarheit**. Sie indizieren zudem, dass die Regeln der KI-VO auch nach dem Digital-Omnibus on AI die Wirtschaft übermäßig belasten. **Besser** wäre jedenfalls eine Ausnahme, die die Regulierung bei **geringem Umfang des Einsatzes von KI** unabhängig von der Unternehmensgröße zurücknimmt.
Art. 1 Abs. 4	Neufassung: Statt Anforderungen an KI-Kompetenz in Art. 4 KI-VO nun Unterstützung der KI-Bildung (AI literacy).	Die Regelung enthält nur eine vage Vorgabe, die nicht beachtet, dass einerseits die EU-Kommission keinen Bildungsauftrag und andererseits die Mitgliedstaaten ohnehin alle nötigen rechtlichen Kompetenzen haben, die KI-Bildung zu fördern (Art. 4 Abs. 1, Art. 5 Abs. 1, 2 EUV). Die Regelung hat **keinen erkennbaren Mehrwert.**
Art. 1 Abs. 5, 7	Berechtigung zur Verwendung personenbezogener Daten i.S. des Art. 9 DSGVO (s. Erw.-Grd. 6) zum KI-Training anstelle des bisherigen Art. 10 Abs. 5 KI-VO (Art. 4a KI-VO n.F.).	Die Regelung definiert **enge Bedingungen**, unter denen ein besondere Kategorien personenbezogener Daten für die Identifizierung von Verzerrungen („bias“) angenommen werden können. Sie stützt sich dabei auf wertungsbedürftige Begriffe („exceptionally process“; „suitable safeguards“). Die Regelung trägt weiter nur begrenzt zur Rechtsklarheit bei.
Art. 1 Abs. 6, 14	Neuregelung der Selbsteinschätzung als Betreiber von Nicht-Hochrisiko-KI (Art. 6 Abs. 4, 49 Abs. 2 KI-VO).	Die Neuregelung **reduziert den Verfahrensaufwand**, weil die Notwendigkeit der **Registrierung in einer EU-Datenbank entfällt.** Sie ist zu begrüßen.

Vorschrift	Inhalt	Stellungnahme
Art. 1 Abs. 8	Anforderungen an die technische Dokumentation von Hochrisiko-KI-Systemen (Art. 11 Abs. 1 UAbs. 2).	Die **Dokumentationsanforderungen** der KI-VO sind insgesamt problematisch: Sie sind sehr umfangreich und **weichen** zudem **vom allgemeinen Marktordnungsrechts ab**, wonach staatliche Stellen nur bei Missbräuchen und konkret drohenden Gefahren in den Markt eingreifen. Die Pflichten ermöglichen vielmehr eine engmaschige Überwachung wie z.B. im Finanzaufsichtsrecht, wo Systemgefährdungen abzuwenden sind. In Hinblick auf Hochrisiko-KI-Systeme ist die neugefasste Regelung samt der Begrenzungen für kleine Unternehmen aber **vertretbar**.
Art. 1 Abs. 9	Größenabhängige Anforderungen an Qualitätsmanagementsysteme (Neufassung Art. 17 Abs. 2 KI-VO)	Die **Regelung ist unklar**, da sie Anforderungen in Bezug auf ein seinerseits wertungsabhängiges Ziel definiert („respect the degree of rigour and the level of protection required to ensure the compliance“).
Art. 1 Abs. 10-15	Verschiedene Änderungen zu Notifizierungen, Konformitätsbewertungen und Praxisleitfäden (Art. 28-30, 43, 50 KI-VO).	Die Änderungen dienen der **Verwaltungsvereinfachung** und Verfahrensbeschleunigung. Insofern sind sie zu begrüßen.
Art. 1 Abs. 16	Überwachung von Praxisleitfäden: Teilhochzonung zur EU-Kommission (Art. 56 Abs. 6 KI-VO).	Die Vorschrift kann – sofern man diese für erforderlich hält – zu einer **effektiveren Aufsicht** beitragen und erhöht für die Marktteilnehmer die Übersichtlichkeit des Aufsichtssystems. Insofern ist sie zu begrüßen.
Art. 1 Abs. 17-19	Ermächtigung zu KI-Reallaboren auf EU-Ebene; weitere Regelungen zu KI-Reallaboren (Art. 57 Abs. 3a KI-VO n.F.).	Die Notwendigkeit von **KI-Reallaboren** (Art. 57 ff. KI-VO) ergibt sich allein daraus, dass KI in der EU einer weitgreifenden speziellen Überwachung unterworfen wird, mit Pflichten, die sich gleichwohl mit anderen Regelungen überschneiden (DSGVO, Verbraucherschutzrecht usw.). Insofern wird der Marktbedeutung der KI je nach Einsatzzweck zu wenig Rechnung getragen, wenn die Risiken grundsätzlich als (zumindest potenziell) systemische Risiken reguliert werden. Die Regelungen zu KI-Reallaboren **belegen** insofern die bestehende **Überregulierung.**
Art. 1 Abs. 20	Neuregelung zur Testung von Hochrisiko-KI-Systemen unter realen	Die Vorschrift steht geradezu **quer zum Regelungsansatz der KI-VO**, der KI-Systeme nach ihrem (potenziell systemischen) Risiko abgestuft reguliert und nur

Vorschrift	Inhalt	Stellungnahme
	Bedingungen außerhalb von Reallaboren (Art. 60a n.F. KI-VO).	Reallabore und diese bisher nur auf mitgliedstaatlicher, regionaler oder lokaler Ebene – d.h. bei begrenzten Auswirkungen im Fall der Risikorealisierung – vorsieht. Die Vorschrift ist zudem **schon jetzt durch die Entwicklung überholt:** In den letzten Jahren wurden KI-Modelle mit allgemeinem Verwendungszweck – wenngleich nicht definierte Hochrisiko-KI-Systeme – im Markt ausgerollt. Die weit verbreitete Nutzung, um die **Systeme unter realen Bedingungen zu testen und zu verbessern,** ist zwar weiterhin **nicht der gesetzliche Regelfall, aber praktisch ein wesentlicher Bestandteil** der Entwicklung bzw. Weiterentwicklung von KI-Systemen.
Art. 1 Abs. 21, 23	Ausnahmen von Vorgaben zu Qualitätsmanagementsystemen für Kleinunternehmen; Beratung (Art. 63 Abs. 1, Art. 70 Abs. 8 KI-VO n.F.).	Auch diese Regelungen sind **notwendig, weil die KI-VO** mit ihrem – ohne Differenzierungen auf potenzielle Systemrisiken ausgerichteten Ansatz – einzelfallabhängig **zu unverhältnismäßigen Anforderungen führen kann.** Anstelle einer Regelung abhängig von der Unternehmensgröße wäre es auch in diesem Kontext **besser**, die Regulierung bei **geringem Umfang des Einsatzes von KI unabhängig von der Unternehmensgröße** zurückzunehmen.
Art. 1 Abs. 25, 26	Zuständigkeitskonzentration für Marktüberwachung auf EU-Ebene; behördliche Kooperation (Art. 75, 77 KI-VO).	Die Änderungen dienen der **Verwaltungsvereinfachung** und können – sofern man diese für erforderlich hält – zu einer **effektiveren Aufsicht** beitragen. Insofern sind sie erneut zu begrüßen.
Art. 1 Abs. 27, 28	Verhaltenskodizes und Leitlinien für Kleinunternehmen (Art. 95, 96 Abs. 1 KI-VO)	Anstelle einer Regelung abhängig von der Unternehmensgröße sollte erneut der **Umfang des Einsatzes von KI-Technologie** im Unternehmen **maßgeblich** sein. Bei allen Unternehmen mit nur geringem KI-Einsatz ist die behördliche Unterstützung durch vereinfachende Leitlinien/Verhaltenskodizes gleichermaßen sinnvoll.
Art. 1 Abs. 29	Erweiterung der Regelungen zu Durchsetzung und Sanktionen auf zusätzliche Kleinunternehmen (Art. 99 KI-VO)	Die Vorschrift regelt weiter nur die **hoheitliche Durchsetzung** durch Behörden der Mitgliedstaaten. Hinsichtlich des zivilrechtlichen Rechtsschutzes ist sie offen. Dies verursacht **Rechtsunsicherheit bezüglich** der Frage, welche **Relevanz** die Anforderungen der KI-VO überhaupt **in Zivilrechtsverhältnissen** haben.

Vorschrift	Inhalt	Stellungnahme
Art. 1 Abs. 30, 31	Hinausschieben des Anwendungsbeginns der KI-VO (Art. 111, 113 KI-VO).	**Die Regelungen sind schon wegen des verfehlten Regulierungsansatzes der KI-VO zu begrüßen. Besser wäre es, die Verordnung würde insgesamt zurückgenommen und eine Neuregelung getroffen, die Risikoschutz und Innovationsförderung besser austariert.**

f) Verordnungsvorschlag über EU-Brieftaschen für Unternehmen (European Business Wallets)

Vorschrift	Inhalt	Stellungnahme
Art. 2	Anwendungsbereich: Bereitstellung und Annahme von Europ. Business Wallets und dafür geeignete Inhaber-Identfizierungsdaten; Einsatz von Europ. Business Wallets.	Die Europ. Business Wallet sollte nicht nur für Unternehmen, sondern auch für sondern auch für Datentransfers im Rahmen von Forschung und Entwicklung nutzbar sein.
Art. 6 Abs. 1	Funktionen von Europ. Business Wallets	Sinnvolle Regelung, insb. soweit auch eine Interaktion zwischen Europ. Business Wallets und European Digital Identity Wallets sicherzustellen ist. Allerdings sollten auch passende Identitätsfunktionen für Forschung und Entwicklung geschaffen werden.
Art. 7 Abs. 2	Anbieter von Europ. Bus. Wallets müssen Sitz in EU haben.	Die Regelung ist vertretbar, um die Rechtsdurchsetzung gegenüber den Anbietern und damit ihre Vertrauenswürdigkeit gewährleisten zu können.
Art. 9 Abs. 1	Nutzung von einem Unternehmen zugewiesenen einheitlichen Kennungen	Neben Unternehmen sollten auch Forschungsinstitutionen eine einheitliche Kennung erwerben können. Die Möglichkeit zum Identitätsmanagement über Europ. Business Wallets dürfte auch im Kontext von Forschung und Entwicklung außerhalb des Unternehmenskontexts relevant sein können.
Art. 9 Abs. 2	Zuweisung einer einheitlichen Kennung aufgrund einer Durchführungs-Rechtsakts	Neben den einheitlichen Kennungen, die von den Mitgliedstaaten nach Vorschriften zur Umsetzung der RL 2017/1132 vergeben werden, sollten auch durch

		internationale Organisationen entwickelte Kennungen wie z. B. der Legal Entity Identifier von GLEIF als unionsweit gültige „einheitliche Kennung“ anerkannt werden können.
Art. 10 Abs. 4	Verzeichnis für Inhaber von European Business Wallets	Außerdem sollte es ein frei einsehbares Verzeichnis geben, das Auskunft über Nutzungsbeschränkungen für Signaturen gibt, die unter Nutzung einer Europ. Business Wallet erteilt werden.

* * *