
Deutsche Industrie- und Handelskammer

Stellungnahme

- **Der Digitalomnibus ist ein richtiger Schritt, verfehlt aber das Ziel, die regulatorische Komplexität der fragmentierten digitalen Gesetzgebung zu reduzieren.**
- **Datenrechtsakte müssen zusammengeführt und widerspruchsfrei gestaltet werden, das gilt insbesondere für KI.**
- **Erforderlich sind allgemeine „safe-harbor“ Normen, die rechtmäßig handelnden Unternehmen Rechtssicherheit verschaffen.**
- **Im Datenschutz gibt es erste Reformschritte, die DSGVO ist in gegenwärtiger Ausgestaltung aber weiterhin ungeeignet für KMU und in Teilen innovationsfeindlich. Dringend notwendige grundlegende Reformen bleiben unberücksichtigt, darunter Regelungen zum internationalen Datentransfer und zum Schadensersatz.**

Vereinfachung – Digitalpaket und -omnibus

Wir bedanken uns für die Gelegenheit zur Stellungnahme zum Digitalomnibus der EU-Kommission (Digital-Omnibus-Verordnung und Digital-Omnibus-Verordnung zur KI).

A. Das Wichtigste in Kürze

Die Vorschläge zum „Digitalen Omnibus“ kommen zur richtigen Zeit. Der über Jahre stetig gewachsene Bestand an Digitalgesetzgebungen belastet Unternehmen zunehmend, schränkt Innovationsfähigkeit ein und sorgt für Rechtsunsicherheiten. Viele der vorgeschlagenen Maßnahmen würden für Vereinfachungen sorgen und sind daher positiv zu bewerten. Gleichzeitig gilt, dass der Omnibus zwar ein wichtiger, aber nur ein erster Schritt zur Verbesserung des Status Quo ist: auf eine gesamtheitliche Harmonisierung des Digital Acquis bleibt weiterhin zu hoffen – zahlreiche Inkonsistenzen, unbestimmte Rechtsbegriffe sowie uneinheitliche Definitionen und Auslegungen bestehen weiterhin.

Unternehmen brauchen effiziente, schlanke und aufeinander abgestimmte Digitalgesetze und dies über alle Branchen und Produkte hinweg. Rechtsunsicherheit und unnötige Komplexität bremsen Innovation – und gefährden am Ende die Wettbewerbsfähigkeit der deutschen Unternehmen. Unternehmen erleben seit Jahren einen massiven Aufbau an Gesetzen für den

digitalen Raum – allein auf europäischer Ebene umfassen digitale Rechtsakte weit über 100 Gesetze¹. Hauptprobleme sind insbesondere Doppelregulierung, Rechtsunsicherheit und unberechenbare Komplexität. Diese führen zu hohem personellen, bürokratischem sowie wirtschaftlichem Aufwand – zu Lasten von Wettbewerbsfähigkeit und Innovation. Für Unternehmen herausfordernd ist zudem das Verhältnis der Digitalgesetze untereinander. Diese sind oftmals gleichrangig, aber anwendungsabhängig - gleichrangig mit sektoraler Spezialisierung oder ergänzend. Nachgelagerte Rechtsordnungen – beispielsweise im Arbeitsrecht – die Schutzfunktionen haben, sind bei der Anwendung der KI-VO ebenfalls zu berücksichtigen.

Zudem ist von zentraler Bedeutung, dass die regulatorischen Vorgaben im Bereich der Datenökonomie in sich konsistent sowie untereinander kohärent ausgestaltet sind und darüber hinaus in Einklang mit bereits bestehenden Regelungen – insbesondere der Datenschutz-Grundverordnung (DSGVO) – stehen. Nur durch eine solche abgestimmte und widerspruchsfreie Regulierung kann gewährleistet werden, dass sowohl rechtliche Klarheit als auch praktikable Umsetzungsmöglichkeiten für Unternehmen und Institutionen geschaffen werden.

Daher braucht es:

- Weniger regulatorische Komplexität sowie Vermeidung von Doppelregulierung. Ausnahmeregelungen für Unternehmen, die bereits nach anderen Fachgesetzen verpflichtet sind und hierdurch bereits vergleichbare oder weitergehende Anforderungen erfüllen.
- Abschaffung der weiterhin zahlreichen unbestimmten Rechtsbegriffe. Es braucht einheitliche Definitionen über alle Digitalgesetze hinweg sowie praxistaugliche Informationsangebote und zuverlässige Leitfäden für Unternehmen.
- Verbesserung der Vorrangregelungen und Harmonisierung der einschlägigen Rechtsordnungen untereinander.
- Schaffung eines besseren Gleichgewichts zwischen Datenschutz und Innovation. Ausnahme der KMU aus der DSGVO, soweit geringes oder normales Risiko durch Datenverarbeitung - mindestens aber KMU-Privileg mit vereinfachten Anforderungen.
- Vereinfachte Datenübermittlung in Drittstaaten bei geringem oder normalem Risiko durch die Datenverarbeitung.

Aus wirtschaftlicher Sicht ist entscheidend, dass der Digital-Omnibus die Unternehmen tatsächlich entlastet, Rechtssicherheit schafft und die Investitionsplanbarkeit erhöht.

B. Bewertung im Einzelnen

Allgemeines

¹ [A dataset of EU legal and policy instruments for the digital world – CEPS](#)

Jeder Digitalrechtsakt sollte über „business readability“ verfügen, d.h. ergänzend zum Gesetzestext Erläuterungen in verständlicher Form erhalten und mit konkreten Use-Cases untermauert werden. Hierfür könnte man sich beispielsweise am Vorgehen beim International Financial Reporting Standard for Small and Medium-sized Entities (IFRS for SMEs) orientieren. Konsequenterweise sollten die Regeln so einfach zu verstehen sein, dass auch ein kleines oder mittelständisches Unternehmen sie ohne externe Dauerberatung rechtssicher umsetzen kann.

Innovationsfreundlichkeit sollte in den Fokus der Aktivitäten der EU-Kommission gestellt werden. Hierzu gehört ein grundlegendes Vertrauen in die gewerbliche Wirtschaft und angepasste Regeln je nach Unternehmensgröße, die z.B. im Rahmen eines „Opt-out-Modells“ KMUs und Small Mid-Caps unter ein vereinfachtes Compliance-Reglement stellen. Im Digitalrecht liegen grundsätzliche Annahmen vor, die Innovationen behindern können, z.B. dass Vollpflichten als Standard gelten, Unternehmen Ausnahmen begründen und Misstrauen statt Vertrauen als Basis vorliegen. Die Beweislast für Ausnahmen liegt bei den Unternehmen und nicht als Beweislastumkehr (Widerspruchsregelung) bei den Behörden. Gerade kleinere Unternehmen ziehen sich von Aktivitäten zurück statt ins Risiko zu geraten. Vollregulierung sollte nur bei klar definiertem Hochrisiko oder auf begründeten Widerspruch der Aufsicht greifen.

Ergänzend braucht es verbindliche Safe-Harbour-Regelungen, die Unternehmen bei Einhaltung definierter Standards vor nachträglicher Haftung und Sanktionen schützen. Wer die festgelegten Regeln einhält, darf darauf vertrauen, rechtmäßig zu handeln – ohne spätere Sanktionen. Es braucht zudem einen gesetzlich verankerten Safe-Harbour-Mechanismus für die Datenweitergabe mit Drittstaatenbezug. Unternehmen müssen bei Nutzung klar definierter Datenkategorien, verbindlicher technischer Schutzmaßnahmen und standardisierter EU-Vertragsmuster darauf vertrauen dürfen, rechtmäßig zu handeln.

Im Omnibus vorgeschlagene Vereinfachungen im Bereich KI

Verschiebung der Umsetzungsfristen

Der Omnibus-Vorschlag sieht eine begrenzte Verschiebung für bestimmte Hochrisiko-Pflichten von maximal 16 Monaten vor, geknüpft an das Vorliegen von Standards und weiteren Unterstützungs-Maßnahmen. Dies deckt sich mit den Forderungen der gewerblichen Wirtschaft, Unternehmen genügend Vorlauf für die Vorbereitung und Umsetzung der Pflichten zu erlauben und die Verpflichtung der Unternehmen mit der Verfügbarkeit von entsprechenden Standards zu koppeln. Gleichzeitig führt der aktuelle Vorschlag jedoch auch zu mehr Rechtsunsicherheit, denn es bleiben nur wenige Monate, bis Annex I greift. Das heißt auch, dass Unternehmen von der Geschwindigkeit des Gesetzgebungsverfahrens abhängig sind. Wird die Verschiebung nicht rechtzeitig verabschiedet, gelten die ursprünglichen Fristen ab August 2026.

In diesem Kontext würden auch ausreichende Übergangsfristen – im Falle von Hochrisiko-KI von einheitlich 12 Monaten – den Unternehmen helfen. Hier ist allerdings weiterhin wichtig, Leitlinien und weitere Maßnahmen praxisnah und anhand konkreter Beispiele unter Einbeziehung der Wirtschaft zu gestalten. Dabei müssen die horizontal geltenden Leitfäden und Standards auch für spezifische KI-Produkte eindeutig anwendbar sein. Auch externe unterstützende digitale Tools – wo möglich passende KI-Lösungen – könnten dabei helfen, schnell, verständlich und insbesondere verbindlich die für Unternehmen relevanten Vorgaben zu erkennen. Ziffer 31, d.h. der Vorschlag einer Fristverschiebung, sollte aus dem Gesamtpaket herausgelöst und im Fast-Track-Verfahren verabschiedet oder inhaltlich nachgeschärft werden um die bereits formulierten Übergangsfristen ohne flexible frühere Eintrittsmöglichkeiten.

KI-Kompetenz

Die unbestimmte Verpflichtung für Unternehmen, KI-Kompetenz sicherzustellen, soll laut Omnibus-Vorschlag abgeschafft werden. Stattdessen sollen Kommission und Mitgliedstaaten die Kompetenzentwicklung fördern. Durch diesen Wechsel der Verantwortlichen können Ressourcen in den Unternehmen freierwerden, wodurch die Anpassung positiv zu bewerten ist. Wichtig ist, dass Kommission und Mitgliedstaaten den neuen Artikel 4 auch unternehmensfreundlich umsetzen und keine neuen Belastungen und Unsicherheiten entstehen. Der bisherige Artikel 4 sorgte bei vielen Unternehmen bereits für große Unsicherheit – die Neuregelung birgt ebenfalls dieses Risiko. Die konkreten Aufgaben, die Mitgliedstaaten und Kommission hierbei künftig zu kommen sollen, müssen daher zeitnah konkretisiert werden. Daneben sollten Maßnahmen ergriffen werden, um KI-Kompetenzen insbesondere im Bereich Aus- und Weiterbildung zu fördern.

Zu berücksichtigen ist jedoch, dass KI-Kompetenzen bei Hochrisiko-Fällen weiterhin durch die Unternehmen im Rahmen ihrer Sorgfaltspflicht gewährleistet sein müssen. Dadurch ist ein kompletter Wegfall der Sicherstellung von KI-Kompetenz durch Unternehmen nicht gegeben.

Dadurch ist ein kompletter Wegfall der Schulungspflicht für Unternehmen nicht gegeben. Generell werden trotz der vorliegenden Änderung KI-Kompetenzen auch in Zukunft Aufgabe der Unternehmen bleiben. Es ist damit zu rechnen, dass Aufsichtsbehörden bei Bußgeldverfahren diese prüfen werden.

Zentralisierte Aufsichtsstrukturen

Die Aufsicht über KI-Systeme auf Basis von GPAI oder jenen, die in sehr großen Online-Plattformen sowie Suchmaschinen eingebettet sind, soll künftig zentralisiert über das KI-Büro erfolgen. Die gewerbliche Wirtschaft fordert schon lange eine möglichst einheitliche Umsetzung der KI-Regeln und Aufsicht, daher wird dieser Ansatz grundsätzlich begrüßt. Entscheidend ist dabei unter anderem, dass ausreichend Ressourcen bereitgestellt werden (u.a. durch die Schaffung neuer Stellen) damit die Aufsicht durch das KI-Büro einen Flickenteppich nationaler Aufsichtsbehörden verhindern und Unternehmen so tatsächlich effektiv unterstützen kann.

Breitere Anwendung von Reallaboren

Die im Vorschlag vorgesehene breite Anwendung von KI-Sandboxen ist positiv zu bewerten. Jedoch führen freiwillige Vereinbarungen zwischen Mitgliedstaaten und der Kommission zu einer Rechtszersplitterung statt einem level playing field, das die EU im europäischen Binnenmarkt herstellen sollte.

Zusammenspiel von AI Act mit anderen Rechtsakten

Das Vorhaben, das Zusammenspiel von AI Act mit anderen EU-Digitalgesetzen besser abzustimmen, deckt sich mit einer der Kernforderungen der gewerblichen Wirtschaft. Allerdings geht der Omnibus-Vorschlag hier nicht weit genug. Im Text ist lediglich von der Erarbeitung von Leitlinien die Rede. Dies muss noch konkretisiert werden. In der DIHK-Stellungnahme vom 14.10.2025 wurden konkrete Stellen, an denen die mangelnde Abstimmung der Regeln besonders klar deutlich wird, hervorgehoben. Vor allem ist wichtig, das jeweilige lex specialis zu präzisieren (Umsetzung der Empfehlung aus dem Draghi-Bericht, wonach die sektorale bzw. spezifischere Vorschrift automatisch Vorrang hätte) bzw. „Lead Acts“ zu definieren, wodurch die Einhaltung der sektoralen Regulierung auch alle Anforderungen aus dem AI Act automatisch mit umfassen würde. Alternativ könnten KI-Themen in sektorale Regulierungen integriert werden.

Die bisherige Formulierung ist jedoch deutlich zu unkonkret und lässt nicht absehen, dass die Probleme in der Koordination von der EU-Kommission hinreichend angegangen werden sollen.

Weitere Vereinfachungen und Erleichterungen

Viele weitere vorgeschlagene Vereinfachungen, wie reduzierte Registrierungspflichten für Betreiber von Systemen, die in Hochrisiko-Bereichen agieren, ohne Hochrisiko zu sein, sind aus Sicht der gewerblichen Wirtschaft zu befürworten.

Allerdings schöpfen die vorgeschlagenen Vereinfachungen ihr Potenzial noch nicht aus, da Unternehmen weiterhin eine vollständige Dokumentation der Prüfung vorhalten müssen. Eine Vereinfachung der Dokumentationsstandards, welche nur auf Anforderung ergänzt wird, wäre eine mögliche Lösung, um wirklich weniger Aufwand zu generieren. Ein weiterer Ansatz könnte sein, dass, sofern kein hohes Risiko besteht, nicht nur Informations-, sondern auch Dokumentationspflichten stärker reduziert werden.

Auch die Ausweitung bestimmter Erleichterungen von KMUs auf Small Mid-Caps ist zu befürworten. Gerade die Förderung dieser Unternehmen, die sich in einer frühen Wachstumsphase ihres Unternehmens befinden, muss gestärkt werden, um die deutsche und europäische Wettbewerbsfähigkeit weiter zu stärken. Diese Small- und Mid-Caps sind besonders von starren Schwellenwerten betroffen, da bereits geringes Wachstum einen abrupten Übergang in die volle Regulierung („regulatorische Klippe“) auslöst. Bei Betrachtung der Größenklassen für Mid-Caps sollte diskutiert werden, die Schwellenwerte (angelehnt z.B. an Auftragsvergaben) auf 1.000 Beschäftigte zu erhöhen. Alternativ wäre eine gleitende Übergangsphase für wachsende

Unternehmen zu erwägen. In allen Fällen ist klar zu definieren, was für SMCs entfällt, um „simplification washing“ zu vermeiden.

Im Bereich der Unterstützung von Unternehmen bei der Anwendung von KI sollte der Fokus auf pragmatische Compliance-Tools wie Checklisten und standardisierte Einstufungshilfen gelegt werden. Neue Vorgaben müssen kompatibel mit etablierten Standards (z.B. ISO 27001, NIS2) sein.

Der Wegfall der Registrierungspflicht für bestimmte KI-Systeme spart Verwaltungsaufwand und ist daher ebenfalls positiv zu bewerten.

Nicht zuletzt sollten offene Schnittstellen gefördert werden, um Vendor-Lock-in zu vermeiden. Im Rahmen des Umgangs mit KI-Sicherheitsvorfällen sollten klare Vorgaben geschaffen werden, um interne Prozesse und Haftungsfragen sauber zu regeln.

Im Omnibus vorgeschlagene Vereinfachungen im Bereich Daten

Generell sind die Ziele der Vereinfachungen im Bereich Daten (Datenzugang für KI, Straffung der Vorschriften, Ziel der Datensouveränität) zu begrüßen, sofern sie nicht mit zusätzlicher Bürokratie verbunden sind. DSGVO, Data Act und AI Act müssen kohärent gestaltet sein.

Zusammenführung der Datenrechtsakte

Die Zusammenführung von vier bestehenden Datenrechtsakten (Data Act, Data Governance Act, Open Data Directive und Free Flow of Non-Personal Data) in ein einziges Instrument, den Data Act, ist grundsätzlich zu befürworten. Insbesondere Probleme wie parallele Rollen, die gleichzeitig auf ein Unternehmen zutreffen können oder konkurrierende Vorschriften, z.B. zum Datentransfer in Drittstaaten, werden dadurch konsolidiert. Gleichzeitig sollte aber die Zusammenführung der Gesetze noch weiter als bisher gedacht werden. Ein Gesetz erzielt keine Erleichterung, wenn vier Logiken bleiben. Materielle Pflichten, Durchsetzungslogiken und Behördenzuständigkeiten bleiben heterogen und müssen auch harmonisiert werden. Der Data Act selbst hätte noch konsequenter verschlankt werden sollen. Vor allem die weitreichenden Berichtspflichten hätten überprüft werden müssen. So müssen Dateninhaber auch ohne eine Beschwerde oder einen anderen konkreten Anlass die zuständige Behörde umfassend über die Umstände einer (gerechtfertigten) Datenzurückhaltung informieren (Art. 4 Abs. 2, 7, 8 sowie Art. 5 Abs. 10, 11 des Data Acts).

Weiterhin bleiben trotz Zusammenführung der Datenrechtsakte noch Unsicherheiten im Zusammenspiel verschiedener Gesetze bestehen. Beispielsweise gibt es bei der Konkretisierung von Begriffen wie „Dateninhaber“, „Datennutzer“ und „Data Processing Services“ noch Lücken. Im Zusammenspiel von Data Act und DSGVO bestehen ungeklärte Fragen zu

Verantwortlichkeiten und Meldepflichten im Spannungsfeld der beiden Verordnungen, z.B. in Bezug auf „Privacy-by-Design“ (DSGVO) und „Access-by-Design“ (Data Act), dem Umgang mit Mischdatensätzen und der Abgrenzung zwischen personenbezogenen und IoT-Daten. Harmonisierungsbedarf besteht auch weiterhin im Zusammenspiel zwischen Data Act und AI Act. Art. 33 legt die Data-Governance-Anforderung innerhalb des Data Acts da, gleichzeitig werden in Art. 10 AI Act die Anforderungen an die Datenqualität, Data Management sowie Data-Governance in Bezug auf Hochrisiko-KI-Systeme festgelegt.

Geschäftsgeheimnisschutz

Der bisherige Mechanismus im Data Act, aufgrund der „hohen Wahrscheinlichkeit eines schweren wirtschaftlichen Schadens durch Offenlegung von Geschäftsgeheimnissen“ die Datenweitergabe zu verweigern, soll laut Vorschlag der EU-Kommission erweitert werden (Art. 4 Abs. 8 (neu) & Art. 5 Abs. 11 (neu)). Auch in Fällen, in denen ein hohes Risiko der unrechtmäßigen Erlangung, Verwendung oder Offenlegung gegenüber Drittländern oder von ihnen kontrollierten Stellen besteht, können nun Daten verweigert werden. Dies ist aus Sicht der Unternehmen zu begrüßen. Kritisch ist dabei, dass unter dem neuen Mechanismus der Dateninhaber selbst dann Daten verweigern kann, wenn Dritte nachweisen, dass sie wirksame Schutzmaßnahmen getroffen haben.

Open Data

Im Bereich Open Data wird im Omnibus-Entwurf vorgeschlagen, öffentlichen Stellen zu erlauben, differenzierte Zugangsbedingungen für offene Daten festzulegen. Sehr große Unternehmen könnten dabei mit höheren Gebühren belegt werden, um die vollständigen Kosten der Datenbereitstellung zu decken und sogar eine Rendite zu erzielen. Dies würde das Ziel einer breiten Wiederverwendbarkeit von Open Data in Europa untergraben. Es drohen individuelle Lizenzbedingungen statt standardisierter Open-Data-Lizenzen, was Inkompatibilitäten schaffen und die Datennutzung einschränken würde.

Weitere Vereinfachungen und Forderungen

Die vorgesehenen Ausnahmen von Cloud-Switching-Vorschriften für KMU sind grundsätzlich zu befürworten, da sie in bestimmten Fällen bürokratische Hürden abbauen.

Mit dem Wegfall des Data Governance Act gibt es keine explizite Definition für Datenaltruismus-Organisationen mehr. Dies sollte daher in Art. 2 Data Act ergänzt werden.

Art. 32c lit. b des Data Governance Act erlaubt Datenvermittlungsdiensten, bestimmte, von ihnen gesammelte Daten für die Weiterentwicklung ihrer eigenen Dienste zu verwenden. Dagegen legt Art. 4 Abs. 11 fest, die Nutzung von Daten für andere Zwecke als ursprünglich vereinbart bedarf der Zustimmung von Nutzern. Hier entsteht ein Widerspruch, der durch den

Digital-Omnibus angegangen werden sollte. Hierdurch sollte die Ausnahme des Art. 32c in den Art. 4 Abs. 11 integriert werden.

Im Omnibus vorgeschlagene Vereinfachungen im Bereich Datenschutz

Die Kommission schlägt verschiedene Änderungen in der Datenschutz-Grundverordnung (DSGVO) vor, die vor allem der Klarstellung und Vereinfachung dienen sollen, ohne das bestehende Datenschutzniveau abzusenken. Die Vorschläge sind grundsätzlich als richtigen Schritt zu bewerten, da sie bestehende Rechtsunsicherheiten verringern und bürokratische Belastungen reduzieren können. Allerdings bleiben viele Anpassungen punktuell, so dass eine durchgehende Harmonisierung weiterhin nicht vollständig gewährleistet ist. Um den Anforderungen der wirtschaftlichen Realität und der technologischen Entwicklung gerecht zu werden, sind daher unter Beibehaltung des Datenschutzniveaus weitergehende Reformen erforderlich.

Dringend notwendige grundlegende Reformen bleiben unberücksichtigt. Insbesondere zentrale Problembereiche wie der Schadenersatz, das Konzernprivileg oder der internationale Datentransfer werden nicht adressiert, obwohl Anpassungen hier für die Wettbewerbsfähigkeit der europäischen Wirtschaft von erheblicher Bedeutung sind.

Für kleine und mittlere Unternehmen (KMU) sollte eine risikobasierte Ausnahme von der DSGVO vorgesehen werden, sofern deren Datenverarbeitung nur ein geringes oder normales Risiko aufweisen. So würde dem risikobasierten Ansatz in der DSGVO konsequent Rechnung getragen, unnötige Bürokratie abgebaut und die Wettbewerbsfähigkeit von KMU gestärkt. Dies würde zu einer Erleichterung der Dokumentations-, Informations- und Nachweispflichten führen.

Wesentliche Erkenntnisse:

- Fehlender durchgängiger risikobasierter Ansatz, so dass Änderungen nur punktuell wirken;
- Privilegierung bei der Verarbeitung pseudonymisierter Daten erforderlich;
- Chance nutzen und Regelungen zu weiteren zentralen Aspekten (Konzernprivileg, Schadenersatz, internationaler Datentransfer) anpassen.

1. Präzisierung des Begriffs „personenbezogene Daten“

Art. 4 DSGVO soll präzisiert werden, indem festgelegt wird, dass Informationen nicht als personenbezogene Daten für eine bestimmte Einrichtung gelten, wenn diese nicht über Mittel verfügt, mit denen die natürliche Person, auf die sich die Information bezieht, mit hinreichender Wahrscheinlichkeit identifiziert werden kann. Diese Änderung steht im Einklang mit der SRB-Entscheidung des EuGH von September 2025.

Diese Änderung soll klarstellen, wann pseudonymisierte Daten als personenbezogene Daten gelten. Demnach gelten in einer bestimmten Einrichtung Informationen dann nicht als personenbezogene Daten, wenn sie nach vernünftigem Ermessen (im Englischen klarer: „reasonably likely“) nicht zur Identifizierung der natürlichen Person, auf die sie sich beziehen, dienen können. Eine solche Datenverarbeitung fällt dann nicht in den Anwendungsbereich der DSGVO. Allerdings sollte eine Klarstellung erfolgen, dass diese Änderung der Definition für jede „verarbeitende Stelle“ gilt. Die derzeitige Formulierung ist diesbezüglich unklar und spricht zum einen vom „Verantwortlichen“, zum anderen von „Einrichtungen“. Zudem stellt sich die Frage, wer die Beweislast dafür trägt, dass eine Identifizierung „nach vernünftigem Ermessen“ (im Englischen klarer: „reasonably likely“) möglich ist oder nicht. Hierfür bedarf es einer klaren Regelung, um neuen Rechtsunsicherheiten entgegenzuwirken.

Über den Vorschlag der Kommission hinaus sollte Art. 5 Abs. 1 lit b DSGVO ausdrücklich die Anonymisierung und Pseudonymisierung als kompatiblen Zweck erfassen. Anonymisierung und Pseudonymisierung stellen keinen eigenständigen, vom Erhebungszweck losgelösten Zweck dar, sondern dienen der Beendigung oder Reduzierung des Personenbezugs und dienen damit der Minimierung datenschutzrechtlicher Risiken vor.

2. KI-Training und KI-Entwicklung

a. Rechtsgrundlage (Art. 88c)

Der Vorschlag beinhaltet die Klarstellung, dass das Verarbeiten von personenbezogenen Daten für KI-Training auf Art. 6 Abs. 1 lit f DSGVO-E – berechtigtes Interesse – gestützt werden kann. Im Übrigen müssen alle Anforderungen der DSGVO einschließlich Transparenz, Datenminimierung und Schutzmaßnahmen eingehalten werden.

Hierbei handelt es sich um eine Klarstellung, die dazu beitragen kann, die Entwicklung von Künstlicher Intelligenz unter Beibehaltung des Grundsatzes der Verhältnismäßigkeit in Europa zu erleichtern und somit Europa als Innovationsstandort zu fördern. Allerdings sollte diese Klarstellung angesichts der technischen Entwicklung sich nicht auf die Verarbeitung in KI-Systemen/KI-Modellen beschränken, sondern technologie-neutral formuliert werden.

b. Art 9 DSGVO

Soweit besondere Kategorien personenbezogener Daten im KI-System- oder KI-Modell gespeichert werden, obwohl die besonderen Kategorien personenbezogener Daten für den Zweck der Verarbeitung nicht erforderlich sind, soll eine Abweichung vom Verbot der Verarbeitung

besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 2 DSGVO unter bestimmten Voraussetzungen zulässig sein. Diese Ausnahme gilt nur unter strengen Bedingungen:

- Der Verantwortliche muss geeignete technische und organisatorische Maßnahmen implementieren, um die Verarbeitung solcher Daten zu vermeiden.
- Werden solche Daten dennoch identifiziert, müssen sie wirksam entfernt werden.
- Wenn die Entfernung unverhältnismäßigen Aufwand erfordert (z. B. weil eine komplette Neuentwicklung des KI-Systems nötig wäre), müssen die Daten zumindest so geschützt werden, dass sie nicht für Ausgaben genutzt, nicht offengelegt und nicht Dritten zugänglich gemacht werden.

Hier wird eine eng begrenzte Ausnahme vom Verarbeitungsverbot für sensible Daten geschaffen, um KI-Entwicklung zu ermöglichen, unter der Voraussetzung besonderer Schutzmaßnahmen. Insbesondere die Möglichkeit, Outputs zu filtern, wird positiv bewertet. Bei einem unverhältnismäßigen Aufwand müssten die Unternehmen ein KI-System nicht neu trainieren, sondern hätten die Möglichkeit, einen Filter zu setzen. So bleibt der Schutz personenbezogener Daten bestehen unter Wahrung der Wirtschaftsinteressen.

Grundsätzlich sollte der Anwendungsbereich des Art. 9 DSGVO nur eröffnet sein, wenn der sensible Charakter des Datums entweder unmittelbar aus dem Datum selbst hervorgeht oder die Verarbeitung auf die Erfassung sensibler Merkmale gerichtet ist. Nicht ausreichend ist, dass sensible Eigenschaften lediglich mittelbar oder zufällig erkennbar sind, sofern diese für den Verarbeitungszweck ohne Bedeutung bleiben. Art. 9 DSGVO sollte daher nur greifen, wenn die Verarbeitung ihrem Zweck nach auf sensitive Merkmale abzielt.

3. Art. 12 Abs. 5, Art. 15 DSGVO Auskunftsanspruch

Der Auskunftsanspruch soll Betroffenen ermöglichen, die Rechtmäßigkeit der Verarbeitung zu überprüfen und ihre Rechte auszuüben. Um die Gefahr des Missbrauchs zu reduzieren, sollten Unternehmen Anfragen dann ablehnen dürfen oder eine angemessene Gebühr verlangen, wenn sie nachweisen können, dass die Anfrage exzessiv oder missbräuchlich ist.

Die Eindämmung missbräuchlicher Auskunftersuchen ist zwingend erforderlich, da strategisch motivierte Anträge in der Praxis zunehmend auftreten. Gerade in langjährigen Arbeitsverhältnissen stellt die rechtskonforme Erfüllung des Auskunftsanspruchs die Arbeitgeber vor erheblichen praktischen Herausforderungen. Daher sollte der Auskunftsanspruch auf personenbezogene Daten, die sich auf die natürliche Privatperson des Arbeitnehmers, beschränken und dabei Ansprüche auf Daten, die durch die Erfüllung der Arbeitnehmerpflichten für den Arbeitgeber generiert werden, ausschließen. Auch das „Recht auf Kopie“ bedarf einer klaren Definition und Einschränkung – etwa durch Ausschluss bereits bekannter oder selbst verfasster Dokumente. Die vorgesehene Möglichkeit einer Ablehnung missbräuchlicher oder exzessiver

Auskunftersuchen ist daher ein wichtiger Schritt. Als belastbares Indiz für Missbrauch oder Exzess sollten etwa unbeantwortet gebliebene Präzisierungsaufforderungen gelten.

Die bisherige grundsätzliche Pflicht zur namentlichen Angabe aller Empfänger (EuGH, Urt. v. 12.01.2023 – C-154/21) führt in der Praxis zu enormen Verwaltungsaufwand, ohne dass der Schutz der Betroffenen verbessert wird. Die Nennung von Empfängerkategorien hingegen reduziert Bürokratie und Rechtsunsicherheit, schützt Geschäftsgeheimnisse, ist für Betroffene verständlicher und entspricht dem tatsächlichen Datenfluss moderner IT-Systeme. Daher sollte es eine gesetzgeberische Klarstellung geben, dass die Nennung von Empfängerkategorien ausreichend ist.

4. Informationspflichten, Art. 13

Insbesondere für kleine Betriebe sollen Informationspflichten nach Art. 13 DSGVO bei Erfüllung bestimmter Voraussetzungen entfallen, nämlich wenn,

- die Beziehung zwischen Betroffenenem und Verantwortlichem klar und überschaubar ist;
- die Verarbeitung nicht datenintensiv und nicht komplex ist;
- es vernünftige Gründe gibt anzunehmen, dass die betroffene Person die Information bereits kennt.

Hiervon gibt es eine Rückausnahme. Die Informationspflichten bleiben bestehen, wenn

- Datenübermittlungen an Dritte erfolgen;
- Daten ins Drittland übermittelt werden;
- Die Verarbeitung zu einem hohen Risiko führt.

Eine Erleichterung bei den Informationspflichten entspricht der jahrelangen Forderung der IHK-Organisation. Soweit die Datenverarbeitung zu keinem hohen Risiko führt, sollten sowohl die Informations- und als auch die Dokumentationspflichten angepasst und reduziert werden, um unnötige Bürokratie zu vermeiden. Daher ist der Vorschlag grundsätzlich positiv zu bewerten. Allerdings schränkt die Rückausnahme zu sehr ein, insbesondere bezogen auf die Datenübermittlung an Dritte und die Drittlandsübermittlung. In der Praxis fallen damit viele Fälle wieder aus der Regelung heraus, obwohl die Verarbeitung zu keinem hohen Risiko führt. So würde z.B. eine Datenübermittlung an einen Auftragsverarbeiter bereits die Rückausnahme auslösen. Daher sollten die Informationspflichten nur bestehen bleiben, wenn die Datenverarbeitung voraussichtlich zu einem hohen Risiko führt. Dies bezieht sich auch auf die Pflicht, ein Verzeichnisse zu führen. Daher ist auch die Regelung aus dem Omnibus IV, die den Art. 30 Abs. 5 DSGVO betreffen, ein wichtiger Schritt in die richtige Richtung, wenn auch isoliert gesehen lediglich eine kosmetische Änderung. Die Erleichterung sollte sich insgesamt durchziehen, damit es zu echten Entlastungen kommt und der risikobasierte Ansatz gewährleistet ist.

5. Art. 33 DSGVO Meldungen von Datenpannen

Die Schwelle für die Meldung an die Aufsichtsbehörde wird angehoben. Eine Meldung soll nur noch erforderlich sein, wenn die Verletzung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen darstellt. Auch die Frist für eine erforderliche Meldung soll auf 96 Stunden erhöht werden. Zudem soll es ein einheitliches Meldeportal (Single-Entry-Point) geben für Meldungen, unter anderem nach der DSGVO, NIS2-Richtlinie, DORA-Verordnung und dem Cyber Resilience Act.

Die Anhebung der Schwelle für Meldungen ist sehr positiv zu sehen. Dies würde dazu führen, dass unnötige Datenschutzverletzungen nicht mehr gemeldet werden müssen. Auch die Verlängerung der Frist ist sinnvoll, allerdings sollte auf Werkstage abgestellt werden, statt auf Stunden. Ein einheitliches Meldeportal wird die Unternehmen durch den Wegfall der Mehrfachmeldungen und Vereinheitlichung der Prozesse jedoch nur entlasten, wenn tatsächlich die Fristen, Definitionen, Vorgaben vereinheitlicht werden.

6. Art. 35 DSGVO Datenschutzfolgenabschätzung

Es sollen EU-weit einheitliche Listen erstellt werden, die verbindliche Vorgaben enthalten, wann die Durchführung einer DSFA erforderlich ist und wann nicht. Diese soll vom Europäischen Datenschutzausschuss erstellt und regelmäßig überprüft werden.

Einheitliche Vorgaben reduzieren die Rechtsunsicherheit für Unternehmen und führen zu mehr Harmonisierung. Hierdurch dürfte auch der Begriff des Risikos geschärft werden, wenn verbindlich festgelegt wird, welche Arten von Verarbeitung als „hochriskant“ gelten und welche nicht. Allerdings muss gewährleistet sein, dass die Listen aktuell gehalten werden. Soweit an einem Überprüfungszyklus von 3 Jahren festgehalten wird, sollte ein Mechanismus vorgesehen werden, der notwendige kurzfristige Änderungen ermöglicht, um so auf aktuelle technische Entwicklungen reagieren zu können.

7. Art. 41a DSGVO-E Privilegierung pseudonymisierter Daten

Die in Art. 41a DSGVO-E vorgeschlagene Privilegierung bei der Verarbeitung von pseudonymisierten Daten ist ein grundsätzlich richtiger Schritt. Allerdings ist die Privilegierung an ein strenges Verfahren geknüpft. Dies birgt die Gefahr, dass eine Privilegierung in der Praxis nicht greifen wird. Zudem bedarf es hierfür eines Durchführungsrechtsaktes der Kommission. Daher ist eine grundsätzliche Regelung zur Privilegierung bei der Verarbeitung von pseudonymisierten Daten erforderlich, um die Verarbeitung dort, wo kein hohes Risiko besteht, zu ermöglichen. Die Privilegierung ist ein ausgewogener Kompromiss zwischen Datenschutz und Wirtschaftsförderung.

8. Cookies

Die bisherige Regelung in der ePrivacy-Richtlinie zu den Cookies wird in die DSGVO integriert, soweit es sich um personenbezogene Daten handelt. Eine Harmonisierung durch das

Zusammenführen der zwei Rechtsakte ist jedoch nicht gegeben, da für nicht-personenbezogene Daten die ePrivacy-Richtlinie relevant bleibt. Das Doppelregime mit unterschiedlichen Voraussetzungen führt in der Praxis zu Rechtsunsicherheiten.

9. Weitere erforderliche Anpassungen

Die vorgeschlagenen Änderungen im Digitalomnibus sind nicht weitgehend genug. Um das Ziel – Vereinfachung des digitalen Rechtsrahmens und Stärkung der Wettbewerbsfähigkeit der europäischen Wirtschaft – zu erreichen, bedarf es weiterer Änderungen:

a. Art. 82 DSGVO – Schadenersatz:

Die aktuelle Rechtslage führt zu erheblicher Unsicherheit und wirtschaftlicher Belastung. Der Schadenbegriff ist unklar und eröffnet Raum für weitreichende Haftungsrisiken. Trotz vieler Urteile vermochte auch die Rechtsprechung noch keine Klarheit zu schaffen – der Gesetzgeber ist gefordert. Gerade im Zusammenhang mit Sammelklagen droht wegen der andauernden Rechtsunsicherheit eine Situation, in der strategische Innovationspotentiale gehemmt werden. Daher sollte eindeutig geregelt werden, unter welchen – nur strikten Voraussetzungen – eine Verbandsklagebefugnis gegeben sein kann. Allein die Bedeutung des Datenschutzrechts kann eine solche Verbandsklagebefugnis nicht rechtfertigen. Das Fehlen einer Erheblichkeitsschwelle und die weite Auslegung des immateriellen Schadens verstärkt diese Problematik.

b. Art 44 ff. DSGVO - Internationaler Datentransfer:

Die global vernetzten Wirtschaftsbeziehungen sind für Unternehmen in Deutschland und Europa von fundamentaler Bedeutung. Dafür ist der internationale Datentransfer essenziell. Da häufig keine Angemessenheitsbeschlüsse der EU bestehen oder diese wie mit den USA nicht dauerhaft sind, bestehen hohe Haftungsrisiken zu Lasten der Unternehmen. Auch die Anforderung, ein „Transfer Impact Assessment“ im Rahmen der Standarddatenschutzklauseln durchzuführen, ist für viele Unternehmen nicht leistbar. Es bedarf schnellerer und belastbarer Angemessenheitsbeschlüsse sowie zentraler Informationen zum Datenschutzniveau in einzelnen Drittstaaten durch die EU-Kommission und Aufsichtsbehörden. Zudem sollten die Voraussetzungen für Ausnahmen nach Art. 49 DSGVO, insbesondere die Einwilligung, praxisnäher ausgestaltet werden.

c. Konzernprivileg

Derzeit werden Konzerngesellschaften als eigenständige datenschutzrechtliche Einheiten behandelt. Dies führt in der praktischen Umsetzung zu erheblichen Schwierigkeiten, da konzerninterne Datenübermittlungen – obgleich organisatorisch notwendig und wirtschaftlich sinnvoll – denselben Anforderungen unterliegen wie Übermittlungen an externe Dritte. In der Praxis besteht ein hoher Bedarf an Datenflüssen innerhalb von Unternehmensgruppen. Um diese realen Strukturen Rechnung zu tragen und zugleich Rechtssicherheit zu gewährleisten, sollte ein Konzernprivileg eingeführt werden, welcher konzerninterne Datenübermittlungen für klar

definierte interne Verwaltungszwecke (z.B. zentrale Personalverwaltung, Finanz- und Rechnungswesenszwecke, Compliance-Überwachung, IT-Sicherheit und Konzernberichterstattung) ermöglicht, ohne dass eine gesonderte Rechtsgrundlage erforderlich ist. Alternativ könnte gesetzlich klargestellt werden, dass konzerninterne Datenübermittlungen grundsätzlich ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f. DSGVO darstellen.

d. Konkludente Einwilligung bei risikoarmen Situationen und Situationen mit normalem Risiko

Um den erheblichen Verwaltungsaufwand im Zusammenhang mit der Einholung und Dokumentation von Einwilligungen zu reduzieren, sollte der Gesetzgeber die Möglichkeit vorsehen, in risikoarmen und in typischen Verarbeitungssituationen mit normalem Risiko konkludente Einwilligungen zuzulassen. Eine solche Regelung würde den tatsächlichen Kommunikations- und Nutzungssituationen Rechnung tragen, in denen betroffene Personen durch ihr Verhalten eindeutig zum Ausdruck bringen, dass sie mit der Verarbeitung einverstanden sind – etwa durch das aktive Bereitstellen von Daten oder die fortgesetzte Nutzung eines Dienstes nach klarer Information. Lediglich bei der Verarbeitung besonderer Kategorien personenbezogener Daten sowie in eindeutig risikobehafteten Verarbeitungskontexten sollte – soweit eine Einwilligung überhaupt als Rechtsgrundlage vorgesehen ist – eine ausdrückliche, zweifelsfrei dokumentierte Einwilligung erforderlich bleiben. Damit würde das Schutzniveau in sensiblen Bereichen gewahrt, ohne dass alltägliche, unkritische Datennutzungen weiterhin durch unverhältnismäßige formale Anforderungen belastet werden.

e. Herstellerhaftung

Vereinzelt wird gefordert die Hersteller mehr in Verantwortung zu nehmen. Die Prinzipien Privacy by Design und by Default sollen dann direkt auch für die Hersteller und Anbieter von Produkten gelten.

Im Omnibus vorgeschlagene Vereinfachungen im Bereich Cybersicherheit

Einheitliche Meldestelle

Der Single-Entry-Point für Sicherheitsvorfälle, der Meldungen erleichtern soll, ist positiv zu bewerten, sofern gleiche Definitionen, gleiche Fristen und gleiche Schwellen gelten. Ein „Report once“ darf kein „Report more“ werden. Gleichzeitig bestehen konkrete Unsicherheiten hervorgerufen durch unterschiedliche Fristen nach DSGVO (72 Stunden) versus NIS2 (24 Stunden), abweichende Definitionen meldepflichtiger Vorfälle, Doppelmeldungen unter DORA/AI Act und unklare Haftungsverteilungen bei Überschneidungen. Dies kann weiterhin zu Mehraufwand, Verzögerungen und Haftungsrisiken führen und sollte daher harmonisiert werden.

Weitere notwendige Anpassungen im Cyber-Bereich, die im Omnibus-Vorschlag fehlen

Über den Single-Entry-Point hinausgehend gibt es noch eine Reihe weiterer Anpassungen, die Unternehmen fordern, die sich aber bisher nicht in den Vorschlägen zum Digital-Omnibus wiederfinden. Hier verweisen wir auch auf unsere Stellungnahme vom 14. Oktober 2025. Konkret handelt es sich um die untenstehenden Punkte.

Im Bereich der Cyberzertifizierungen könnten insbesondere kleine und mittlere Unternehmen (KMU) davon profitieren, wenn es abgestufte Zertifizierungsanforderungen gibt. Ohne eine solche abgestufte Lösung wird aktuell die Gefahr gesehen, dass große Unternehmen von allen Partnern in ihrer Lieferkette die höchste Zertifizierungsstufe verlangen müssen, um selbst zertifiziert zu werden. Das würde insbesondere KMU im Wettbewerb benachteiligen, da sie die hohen Anforderungen oft nicht erfüllen können.

Das Ziel der NIS2 – die Schaffung eines einheitlich hohen Cybersicherheitsniveaus innerhalb der EU – droht verfehlt zu werden. Da es sich bei NIS2 um eine Richtlinie handelt, werden die regulatorischen Anforderungen in den jeweiligen EU-Ländern unterschiedlich ausgelegt und umgesetzt. In der Folge ist es für international agierende Unternehmen beispielsweise unklar, ob eine Meldung in jedem Land erfolgen muss und wie die Länder untereinander kommunizieren. Eine einheitliche Umsetzung der NIS2-Richtlinie wäre dringend notwendig.

Damit Sicherheitsvorgaben effizient und praxisnah umgesetzt werden können, sollten die Prozesse der Zusammenarbeit zwischen Behörden sowie zwischen Behörden und Unternehmen von Anfang an klar geregelt und abgestimmt sein. Ein gut abgestimmtes Zusammenspiel der Behörden ermöglicht hingegen eine gezielte und wirksame Kommunikation mit den Unternehmen, etwa durch frühzeitige Warnhinweise oder abgestimmte Anforderungen. So sollten vor allem Marktüberwachungsbehörden gehalten sein, im Rahmen der Aufgabenerfüllung ihr Ermessen so weit wie möglich mit dem Ziel der Innovationsförderung auszuüben.

Die EU-Kommission sollte sicherstellen, dass Unternehmen einen konkreten und spürbaren Nutzen aus der Zusammenarbeit mit staatlichen Sicherheitsbehörden und europäischen Institutionen ziehen können. Die für Unternehmen zentralen Anlaufstellen müssen im Sinne einer bestmöglichen Innovationsförderung für effektive sowie praxistaugliche Strukturen und Angebote sorgen. Ein zentraler Aspekt ist dabei die Etablierung eines effektiven Rückkanals für gemeldete Sicherheitsvorfälle.

C. Ergänzende Informationen

a. Ansprechpartner mit Kontaktdaten

Jonas Wöll

Referatsleiter Digitaler Binnenmarkt, EU-Verkehrspolitik, Regionale Wirtschaftspolitik

Tel: +49 151 11314837

E-Mail: woell.jonas@dihk.de

Kei-Lin Ting-Winarto

Leiterin des Referats Datenschutz

Rechtsanwältin (Syndikusrechtsanwältin)

Tel: +49 30 20308-2717

E-Mail: ting-winarto.kei-lin@dihk.de

Jennifer Evers

Referatsleiterin Alternative Konfliktlösung (Schiedsgerichtshof), Recht der digitalen Wirtschaft und Legal Tech

Rechtsanwältin (Syndikusrechtsanwältin)

Tel: +49 30 20308-2719 / Mobil: +49 1511 1332 151

E-Mail: evers.jennifer@dihk.de

b. Beschreibung DIHK

Wer wir sind:

Unter dem Dach der Deutschen Industrie- und Handelskammer (DIHK) sind die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich die DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein. Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zum Gesamtinteresse der gewerblichen Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.

Grundlage unserer Stellungnahmen sind die wirtschaftspolitischen Positionen und beschlossenen Positionspapiere der DIHK unter Berücksichtigung der der DIHK bis zur Abgabe der Stellungnahme zugegangenen Äußerungen der IHKs und ihrer Mitgliedsunternehmen.

Darüber hinaus koordiniert die DIHK das Netzwerk der 150 Auslandshandelskammern, Delegationen und Repräsentanzen der Deutschen Wirtschaft in 93 Ländern.

Die DIHK ist im Transparenzregister der Europäischen Union unter der Nummer 22400601191-42 registriert.