Brüssel, 14. Oktober 2025

Deutsche Industrie- und Handelskammer

Stellungnahme

DIHK-Stellungnahme zum geplanten Vereinfachungspaket für den Digitalbereich

Wir bedanken uns für die Gelegenheit zur Stellungnahme zu den Omnibusvorschriften für den Digitalbereich. Die Stellungnahme beruht auf den uns zugegangenen Äußerungen der Industrie- und Handelskammern (IHKs), den Erkenntnissen, die innerhalb der IHK-Organisation sowie im Austausch mit Mitgliedsunternehmen gesammelt wurden, sowie auf den Wirtschaftspolitischen Positionen der DIHK. Sollten uns noch weitere Rückmeldungen, zu von uns bisher nicht berücksichtigten Äußerungen zugehen, werden wir die Stellungnahme ergänzen.

- Vereinfachung und Innovationsfähigkeit in den Vordergrund stellen
- Kohärenz der Regulierung im gesamten Digitalbereich sicherstellen – einschließlich des Datenschutzes
- Cyberresilienz stärken und regulatorische Inkonsistenzen abbauen
- Definitionen in allen digitalen Rechtsakten schärfen, vor allem bei AI Act und Data Act

A. Das Wichtigste in Kürze

In der vergangenen Legislaturperiode wurde eine Reihe von Digitalregulierungen durch die EU verabschiedet – von digitalen Märkten über KI bis hin zu Daten. Während dies in einigen wenigen Fällen für die lang angemahnte Rechtssicherheit gesorgt hat, ist durch die Vielzahl an neuen, oft nicht miteinander abgestimmten Regeln auch ein erhebliches Maß an neuer Rechtsunsicherheit entstanden. Ein Großteil der Unternehmen, insbesondere KMU, sieht sich einer Flut an komplexen Regeln gegenübergestellt: Während Bürokratie und Pflichten stetig ansteigen, droht die Innovationsfähigkeit nachzulassen.

In diesem Kontext bewertet die deutsche gewerbliche Wirtschaft die Initiative der EU, mit dem „Digital-Omnibus“ ein Vereinfachungspaket auf den Weg zu bringen, grundsätzlich ausgesprochen positiv. Damit alle Unternehmen davon profitieren, müssen zwei Punkte im Vordergrund stehen: Vereinfachung und Innovationsförderung.

Vereinfachung: Die Unternehmen benötigen dringend ein kohärentes Regelwerk sowie verlässliche Rahmenbedingungen. Die Vielzahl von Digitalregulierungen muss praxistauglich zusammengeführt werden. Auch bedarf es klarer Strukturen und Zuständigkeiten im Bereich der Marktüberwachung, um Doppelzuständigkeiten und Überregulierung zu verhindern bzw.

DIHK | Deutsche Industrie- und Handelskammer
Besucheranschrift: Breite Straße 29 | 10178 Berlin-Mitte | Postanschrift: DIHK | 11052 Berlin
Tel. 030-20308-0 | Internet: www.dihk.de

einzudämmen. Denn bislang erscheint es, als stünden Kontrolle und Einhaltung gesetzlicher Vorgaben derart im Vordergrund, dass der Gesamtbereich der digitalen Wirtschaft, des digitalen Binnenmarktes von der EU mehr als Gefahr und Drohung wahrgenommen wird, während der Draghi-Bericht deutlich auf die Möglichkeiten und Chancen hingewiesen hat. Es bleibt zu hoffen, dass mit dem geplanten Digital-Omnibus – als echtes Vereinfachungspaket – auf die Unternehmen ein weiterer schlanker Regulierungskomplex zukommt, der den großen Ankündigungen von regulatorischer Vereinfachung, Harmonisierung von Vorschriften und Vereinheitlichung von Begriffsdefinitionen, Förderung von Innovation und Wettbewerbsfähigkeit sowie Abbau von Bürokratie gerecht wird.

Innovationsförderung bedeutet konkret, Freiräume für Unternehmen in der digitalen Wirtschaft zu schaffen. So sollten vor allem Marktüberwachungsbehörden gehalten sein, im Rahmen der Aufgabenerfüllung ihr Ermessen so weit wie möglich mit dem Ziel der Innovationsförderung auszuüben. Die für Unternehmen zentralen Anlaufstellen müssen im Sinne einer bestmöglichen Innovationsförderung für effektive sowie praxistaugliche Strukturen und Angebote sorgen. Bei unklaren Abgrenzungen sollten die Grundsätze der Verhältnismäßigkeit und Innovationsförderung anwendet werden.

Eine wesentliche Rolle auf nationaler Ebene können dabei Unterstützungsangebote wie der neue KI-Service Desk der Bundesnetzagentur spielen, der Unternehmen helfen soll, die komplexen Anforderungen der europäischen KI-Verordnung effizient und praxisnah zu erfüllen. Auch hier darf der Fokus am Ende nicht auf dem Aufbau von Verwaltungsstrukturen liegen, sondern auf für die Unternehmen in der Praxis tatsächlich tauglichen Bedingungen. Wichtige wirtschaftliche und personelle Ressourcen sollten dafür genutzt werden können, die unternehmenseigene Digitalisierung entscheidend voranzubringen, statt sich ihr zu verschließen oder nur zögerlich aktiv widmen zu können, aus Sorge nicht rechtskonformen Handelns.

Die digitale Transformation droht an Deutschland und der EU vorbeizurauschen, wenn nicht endlich für wirtschafts- und innovationsfreundliche Rahmenbedingungen, mit schlanken und insbesondere schnellen Strukturen und klarer Orientierung durch eine konsistente und widerspruchsfreie Digitalregulierung für Unternehmen gesorgt wird.

Von zentraler Bedeutung ist vor allem, 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.

Dabei kommt es jetzt auch auf eine schnelle Umsetzung der Vorhaben an – denn die technologische Entwicklung wartet nicht auf eine Regulierungsbehörde, was dazu führt, dass bestehende Vorschriften schon jetzt oft nicht mehr zeit- bzw. sachgemäß sind.

Im vorliegenden Papier werden eine Reihe zentraler Maßnahmen vorgeschlagen, um die Wettbewerbsfähigkeit der EU-Digitalwirtschaft zu stärken. Im Fokus steht dabei insbesondere eine bessere Abstimmung der Rechtstexte aufeinander, mehr Rechtssicherheit sowie Abbau des bürokratischen Aufwands für Unternehmen.

B. Bewertung im Einzelnen

Vorbemerkung

Unternehmen, insbesondere KMU, stehen einem Dschungel an Digitalregulierungen gegenüber und sind insbesondere hohem bürokratischen Aufwand, z.B. durch Meldepflichten, ausgesetzt, der statt eines verlässlichen Rahmens zu großer Rechtsunsicherheit geführt hat. Rechtliche Unsicherheiten sind laut DIHK-Digitalisierungsumfrage 2025 bei der Digitalisierung für fast jedes dritte Unternehmen eine Herausforderung. Insbesondere für KMU ist die Vielzahl an unterschiedlichen Digitalrahmen zunehmend eine Herausforderung. Doppelregulierungen sowie analoge, dezentrale und komplexe Prozesse sorgen für hohen technischen, personellen und finanziellen Aufwand. Oftmals führen bereits überkomplexe Formulierungen in den Rechtstexten dazu, dass wichtige Pflichten übersehen oder falsch ausgelegt werden. Die Digitalgesetzgebung in der EU muss dringend vereinfacht und harmonisiert werden.

Geplante Vereinfachungen sind grundsätzlich zu begrüßen und können weitreichende positive Folgen und Effekte für die Unternehmen haben.

Ziele des Digital-Omnibus sollten vor allem sein: Technologieoffenheit, Innovationsförderung, Bürokratieabbau, Stärkung des digitalen Binnenmarkts, einheitliche Anwendung, Harmonisierung und Umsetzung von Vorschriften in der EU bestenfalls einhergehend mit einer Reduzierung an Vorschriften insgesamt, weniger Fragmentierung, einheitliche Definitionen sowie Auslegung von Begrifflichkeiten und damit in Summe ein Erhöhen der Rechtssicherheit für Unternehmen. Mit Blick auf Cybersicherheit wird die Notwendigkeit einer erhöhten Wachsamkeit gesehen. Zudem sollten auch Meldepflichten vereinfacht und beispielsweise durch zentrale Meldeportale ermöglicht werden.

Wichtig ist es, dass die Vereinfachungen und etwaigen neuen Regeln mit frühzeitigen Unterstützungsangeboten für die Unternehmen einhergehen – beispielsweise praxisorientierte Leitfäden insb. für KMU sowie mögliche Informationskampagnen und Beratungsleistungen. Auch dem potenziellen Risiko von Rechtsunsicherheit für die Unternehmen während der Umsetzungsphase der durch den Digital-Omnibus sodann auf die Unternehmen zukommenden Neuerungen muss ebenfalls angemessen Rechnung getragen werden. Auch sollten wirtschaftliche Belastungen soweit möglich minimiert werden. Der Erhalt der Marktfähigkeit darf insbesondere für KMU nicht mit unverhältnismäßig hohen Investitionskosten verbunden sein.

Relevant ist zudem, auf mehr Spezifität bei der Anwendung von Vorschriften zu achten und beispielsweise differenziert nach Sektoren zu handeln, um besonders regulierte Branchen nicht noch stärker zu belasten und um Vereinfachungen gezielt einsetzen zu können.

Forderungen nach One-in-one-out bzw. One-in-two-out Regeln sind grundsätzlich zu begrüßen, müssen aber konsequent auf EU- und nationale Regeln gleichermaßen angewandt werden. Im Sinne der „good governance" sollten ohnehin nur dann neue Regulierungen eingeführt werden, wenn diese mit spürbaren Erleichterungen für die Wirtschaft verbunden sind.

Cybersicherheit und Cyberresilienz

Allgemeine Punkte

Unternehmen haben umfangreiche Cybersicherheitsanforderungen einzuhalten. Diese müssen nicht nur technisch umgesetzt, sondern auch organisatorisch verankert werden. Dazu gehört auch, das Bewusstsein für die Bedeutung von IT-Sicherheit bei den Mitarbeitenden der Unternehmen kontinuierlich zu schärfen und durch entsprechende Schulungsangebote zu etablieren. Vorgenanntes bindet sowohl personelle als auch finanzielle Ressourcen und bedarf entsprechender Vorbereitung. Zugleich gilt es die eigene Cyberresilienz sicherzustellen und kontinuierlich zu stärken.

Daher sollten ausreichend lange Übergangsfristen vorgesehen werden, damit Unternehmen die oft komplexen Anforderungen, die sich für sie aus Regularien der Cybersicherheit und Cyberresilienz ergeben, technisch, personell und organisatorisch in ihre Prozesse integrieren können. Nur so kann eine flächendeckende und nachhaltige Verbesserung der Cybersicherheit sowie Resilienz erreicht werden, ohne einzelne Akteure zu überfordern oder aus dem Markt zu drängen.

Praxistaugliche Zertifizierungsprozesse

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.

Mit abgestuften Zertifizierungsanforderungen könnte erreicht werden, dass größere Unternehmen, die gesetzlich strengere Anforderungen erfüllen müssen (z. B. durch die NIS2-Richtlinie), diese Anforderungen auch dann weiterhin erfüllen können, wenn sie mit kleineren Dienstleistern zusammenarbeiten, die niedrigschwelliger zertifiziert sind. Voraussetzung dafür wäre, dass diese kleineren Dienstleister eine vereinfachte, aber offiziell anerkannte Zertifizierung

vorweisen können – etwa die VdS-10000 – und diese in den Gesamtzertifizierungsprozess des größeren Unternehmens eingebunden wird.

Inkonsistenzen zwischen Cybergesetzen abbauen

Neben einzelnen Abschnitten von Cybergesetzen sind vor allem deren Wechselwirkungen untereinander oftmals eine Herausforderung für viele Unternehmen. Gesetze wie CRA, DORA und NIS2 decken ähnliche Fälle ab, was zu Dopplungen und Verwirrung bei Unternehmen führt. Beispielsweise sind die Anforderungen für Vulnerabilitätsmanagement und dem Berichten von Vorfällen im CRA gedoppelt mit den Resilienz-Anforderungen unter DORA. Auch bei NIS/NIS2 können Dopplungen mit DORA, z.B. im Falle der Registrierung bei nationalen Cybersicherheits-Behörden, vorkommen.

Für bestimmte Unternehmen, beispielsweise Telekommunikationsanbieter, gelten besonders viele Meldepflichten, unter anderem durch NIS2 und CRA, die jeweils unterschiedliche Anforderungen, Meldefristen und Schwellenwerte aufweisen. Bei einem IT-Sicherheitsvorfall mit Datenschutzverletzung entstehen auch Meldepflichten gemäß der DSGVO.

Eine deutliche Vereinfachung für Unternehmen wäre eine koordinierte, EU-weite Meldemöglichkeit, z. B. über die europäische Cybersicherheitsbehörde ENISA. Gleichzeitig sollten auch die Anzahl der Meldungen (z. B. nach CRA und NIS2) kritisch überprüft werden und eine Harmonisierung sowie Klarstellung bzgl. der jeweiligen Vorrangigkeit der betroffenen Richtlinien das Ziel sein.

Daher sollten die entsprechenden Gesetze einer intensiven Überprüfung unterzogen werden, insbesondere mit Blick auf Berichts- und Meldepflichten, wie die hieraus entstehenden Daten genutzt werden und wie die gleiche oder eine höhere Effektivität der Cybersicherheit mit weniger Datenpunkten erreicht werden kann.

NIS2-Richtlinie

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. Ebenso wird die NIS2 unterschiedlich schnell umgesetzt. So ist es für international agierende Unternehmen beispielsweise unklar, ob eine Meldung in jedem Land erfolgen muss und wie die Länder untereinander kommunizieren. Diese Fragmentierung besteht auch bei den unterschiedlichen Ansätzen bei der Klassifizierung von Unternehmen, den branchenspezifischen Anwendungsbereichen sowie festgelegter Schwellenwerte für Unternehmen. Dadurch können Unternehmen je nach Land unterschiedlichen Compliance Anforderungen unterliegen.

Eine zentralisierte sowie standardisierte und abgestimmte Umsetzung der NIS2-Richtlinie wäre dringend notwendig. Zumindest sollten die EU-Länder bei der Umsetzung insbesondere auf einheitliche Definitionen, Schwellenwerte sowie harmonisierte Meldepflichten und Sanktionen achten.

Zusammenarbeit zwischen Behörden verbessern

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.

Besonders wichtig ist das vor dem Hintergrund, dass verschiedene Sicherheitsgesetze von unterschiedlichen Behörden verantwortet werden. Diese müssen sich wiederum mit weiteren sektorbezogenen Aufsichtsstellen sowie mit regionalen Behörden – etwa denen der Bundesländer in Deutschland – abstimmen. Bei unklaren Abgrenzungen sollten die Grundsätze der Verhältnismäßigkeit und Innovationsförderung anwendet werden. Ohne klare und koordinierte Abläufe besteht die Gefahr von Doppelarbeit und unnötigem Aufwand für Unternehmen, zum Beispiel durch mehrfach erforderliche Meldungen desselben Vorfalls.

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. Alle Maßnahmen sollten darauf ausgerichtet sein, das Sicherheitsniveau in den Unternehmen zu erhöhen und deren eigene Schutzmaßnahmen sinnvoll zu unterstützen.

Mehrwert für Unternehmen schaffen

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 – insbesondere an das Bundesamt für Sicherheit in der Informationstechnik (BSI) und vergleichbare Stellen in anderen Mitgliedstaaten. Unternehmen sollten im Gegenzug gezielte Lageinformationen sowie praxisnahe Handlungsempfehlungen erhalten, um ihre Sicherheitsmaßnahmen verbessern zu können.

Ein solcher kooperativer Ansatz zwischen Staat und Wirtschaft ist bereits in Teilen etabliert, zum Beispiel in Deutschland im Rahmen von UP KRITIS für kritische Infrastrukturen oder durch die Allianz für Cybersicherheit. Diese bestehenden Strukturen sollten weiter ausgebaut und auf weitere Bereiche übertragen werden – idealerweise als umfassendes Unterstützungsnetzwerk für Unternehmen.

Vertretung der DIHK | Deutsche Industrie- und Handelskammer bei der EU
19 A-D, Avenue des Arts | B-1000 Bruxelles
Tel. +32 2 286-1611 | Fax +32 2 286-1605 | Internet: www.dihk.de

AI Act und begleitende Maßnahmen

Die deutsche Wirtschaft setzt vermehrt auf den Einsatz von KI. In der DIHK-Digitalisierungsumfrage 2025 haben 70% der Unternehmen angegeben, KI im Einsatz zu haben oder den Einsatz innerhalb der nächsten drei Jahre zu planen. Vor dem Hintergrund der globalen Wettbewerbsfähigkeit und dem Wunsch nach digitaler Souveränität sind starke KI-Projekte aus Deutschland und Europa unabdingbar. Das macht es hochrelevant, alle bestehenden Handlungsmöglichkeiten zu nutzen, um die Umsetzung der KI-VO so wirtschafts- und innovationsfreundlich wie möglich zu gestalten.

Daher begrüßen wir grundsätzlich das mit dem AI Act verbundene Ziel, einen klaren, einheitlichen Rechtsrahmen für die Entwicklung und Nutzung von KI in der EU zu schaffen.

Aktuell erschweren jedoch die hohe Komplexität des Regelwerks, die Klassifizierung zahlreicher Anwendungsfälle in den Hochrisikobereich, unklare Begriffsdefinitionen und die Normenkonkurrenz von DSGVO-, Urheberrechts- und Cybersicherheitsanforderungen die praktische Umsetzung in vielen Unternehmen. Um den AI Act praxistauglich und innovationsfördernd implementierbar zu machen, braucht es realistische Umsetzungszeiträume, Rechtsklarheit, Unterstützung für KMU und gute Voraussetzungen für eine Integration in bestehende Compliance-Strukturen. Ebenso signalisieren die Unternehmen einen großen Bedarf an Rechtssicherheit. Daher sollten die praktische Handhabbarkeit und Verständlichkeit bei der Umsetzung besonders berücksichtigt werden. Zugleich sollte es Unternehmen möglich sein, sich auch ohne aufwendige externe Beratung oder hohe Kosten regelkonform zu verhalten.

KI und Daten

Eine Kohärenz sollte für alle Stufen der Datenverarbeitung mit KI sowie für eine rechtssichere Nutzung von Datenräumen herbeigeführt werden. Notwendig ist eine eindeutige und praktikable Regelung zur Verwendung personenbezogener Daten beim Training von KI. Hier sollte möglichst in den Artikeln der DSGVO oder in den Erwägungsgründen festgelegt werden, wie Betroffenenrechte (z. B. Auskunft, Berichtigung und Löschung) und Rechtsgrundsätze (z. B. der Datenminimierung) rechtssicher umgesetzt werden können.

So fordern z.B. die Performanzanforderungen des Art. 15 des AI Acts für Hochrisiko-KI-Systeme ein angemessenes Maß an Genauigkeit. Dazu können auch sensible Daten notwendig sein, deren Nutzung nicht im Einklang mit der DSGVO steht. Hierfür braucht es neue Ansätze wie z.B. rechtssichere Datenräume. Das Verhältnis zu Art. 5 Abs. 1 lit. b) HS 2 (Alt.2) „wissenschaftliche Zwecke“ sollte geklärt und hierbei auch privatwissenschaftlichen Unternehmen eine gesicherte Datenverarbeitung ermöglicht werden. Auch fehlt es derzeit an klaren Maßgaben zu rechtssicheren Anonymisierungsverfahren. Eine hohe Datenverfügbarkeit wird nicht erreicht, solange beim Entfernen des Personenbezuges für die datenschutzrechtlich verantwortlichen Unternehmen hohe Unsicherheiten bleiben. Es braucht ein Mindestmaß an Klarheit über das zu

gewährleistende Maß an Anonymität und praktische Vorgaben zum konkreten Vorgehen beim Herstellen eines belastbaren Anonymitätsgrads.

Der AI Act will Diskriminierung beim Einsatz von KI-Systemen reduzieren. Hierzu braucht es entsprechende Trainingsdaten. Gemäß Art. 9 der DSGVO dürfen besonders geschützte Daten nur mit expliziter gesetzlicher Ausnahme verarbeitet werden. Art. 10 Abs. 5 des AI Acts stellt eine solche Ausnahme dar – allerdings nur für Hochrisiko-KI-Systeme. Diese Ausnahme sollte mit entsprechenden Schutzmaßnahmen auf KI-Modelle mit allgemeinem Verwendungszweck (GPAI-Modelle) und Nicht-Hochrisiko-Systeme ausgeweitet werden.

Regulatorische Unsicherheit und Unterstützung bei der Umsetzung

Vielfach herrscht insbesondere bei Anwendung des AI Acts noch regulatorische Unsicherheit. Unabdingbar ist es, Unternehmen bei der Umsetzung eng zu unterstützen – zum einen durch Leitlinien, Service Desks und vergleichbare Angebote. Speziell die Leitlinien zur Umsetzung der Hochrisiko-Vorschriften (Art. 6 Abs. 5 KI-VO) sollten möglichst zeitnah und unbedingt vor der vorgesehenen Frist am 02. Februar 2026 veröffentlicht werden, um Unternehmen genügend Vorlauf für die Vorbereitung und Umsetzung der Pflichten zu erlauben. Wichtig wird die Auflistung von praktischen Beispielen sein, die möglichst viele relevante Anwendungen aus verschiedenen Sektoren umfassen sollte. Dabei müssen die horizontal geltenden Leitfäden und Standards auch für spezifische KI-Produkte eindeutig anwendbar sein. Gesetzliche Vorgaben, Standards und Normen müssen zu den Regeln anderer EU-Rechtsakte konsistent, kohärent und komplementär sein. Eine geringe Anzahl sollte die wichtigsten Anforderungen abdecken.

Vor allem kleine und mittlere Unternehmen (KMU) haben nicht immer ausreichende Rechtskompetenzen und benötigen pragmatische Unterstützung in der Umsetzung des AI Acts. Hierfür müssen das AI Office und der AI Act Service Desk praxisnahe, interdisziplinäre Kompetenzen aufbauen. Umfassendere, komplexere Konkretisierungen sollten durch eigene oder zertifizierte externe unterstützende digitale Tools – wo möglich passende KI-Lösungen – dabei helfen, schnell, verständlich und insbesondere verbindlich die für sie relevanten Vorgaben zu erkennen. Es braucht einen Katalog mit KMU-Anwendungen und klaren Risikoeinstufungen, Self-Assessment-Tools für KMU und Safe-Harbor-Regelungen.

Eine erfolgreiche Einhaltung der Vorschriften erfordert die rechtzeitige Verfügbarkeit dieser Leitlinien, delegierten Rechtsakte und Verhaltenskodizes. Derzeit sind diese entweder verspätet oder noch nicht ausreichend ausgearbeitet. Der Druck, enge Fristen einzuhalten, hat dazu geführt, dass oftmals Interessengruppen nicht genügend eingebunden und Vorschriften nicht hinreichend ausgearbeitet wurden. Darüber hinaus führt diese Diskrepanz zu einem unpraktikablen und, was die Unternehmen betrifft, oft unzumutbaren Zeitplan, der sie zwingt, die Anforderungen zu erfüllen, bevor überhaupt die notwendige Klarheit besteht.

Das „Living repository to foster learning and exchange on AI literacy" zeigt, wie konkrete Umsetzungsunterstützung für Unternehmen aussehen kann. Diese Beispiele sollten kontinuierlich erweitert und für Unternehmen verbindliche Rechtssicherheit schaffen.

Gleichzeitig ist auch ein realistischer Umgang mit Umsetzungsfristen elementar. Wenn jene Teile des AI Acts, die an das Vorhandensein bestimmter Standards und Strukturen geknüpft sind oder Leitlinien zur Konkretisierung der jeweiligen Anforderungen erfordern, in Kraft treten, bevor die entsprechenden Regelwerke verabschiedet und Standards sowie Strukturen vorhanden sind, sorgt dies für große Rechtsunsicherheit in der Wirtschaft. Deshalb sollten neue gesetzliche Vorgaben – insbesondere wenn sie Verpflichtungen für Unternehmen begründen – erst dann in Kraft treten, wenn die für eine erfolgreiche Umsetzung durch die Unternehmen ebenfalls vorgesehenen bzw. notwendigen Leitlinien und technischen Standards rechtzeitig veröffentlicht wurden. Ebenfalls sollte aufgrund schneller technologischer Entwicklungen eine gewisse Flexibilität und Anpassungsfähigkeit der Regulierung gewährleistet sein. Zudem bedarf es ausreichender Übergangszeiten, damit sich Unternehmen auf die neuen Anforderungen vorbereiten und erforderliche Maßnahmen rechtzeitig treffen können. Einzelne Unternehmen fordern auch weitergehende Maßnahmen wie einen „Stop the Clock"-Mechanismus für bereits laufende Fristen bzw. Umsetzungsphasen oder eine Streichung gewisser bereits vorhandener Regeln (Art. 8-27) für Hochrisiko-KIs.

Bestehende Regulierungen sollten einer kritischen Evaluierung unterzogen werden, in deren Rahmen auch geprüft werden sollte, welcher Regelumfang weiterhin Bestand hat und wo ein Weglassen gewisser Regelungen bestehende Doppel- bzw. Überregulierung reduzieren könnte, da bereits über andere vorhandene Gesetze der zu erfassende Sachverhalt ausreichend geregelt ist. Soweit möglich sollten sodann Potenziale genutzt werden, um insbesondere KMU sowie Start-Ups regulatorisch zu entlasten.

Definitionen und Begrifflichkeiten im AI Act

Um den Forderungen nach Rechtsklarheit und Einheitlichkeit nachkommen zu können, bedarf es auch der Evaluierung und Vereinheitlichung von Begrifflichkeiten. Uneinheitliche Definitionen und Auslegungen führen bereits jetzt zu großer Rechtsunsicherheit. Zur Veranschaulichung der Problematik soll nachfolgende Auswahl an Beispielen dienen:

Präzisierung der Definition von „Sicherheitsbauteil" (Art. 3 Nr. 14): Es sollte klargestellt werden, unter welchen Bedingungen KI-Komponenten in kritischen Infrastrukturen (z. B. Drucksensoren in Wasserversorgungssystemen, autonome Kontrollroboter in Kraftwerken, intelligente Kameras mit Bilderkennung) als „Sicherheitsbauteil" (Art. 3 Nr. 14 KI-VO) gelten. In diesem Zusammenhang ist ebenfalls zu spezifizieren, was in der Legaldefinition von „Sicherheitsbauteil" unter der Erläuterung „Bestandteil eines Produkts oder KI-Systems" zu verstehen ist.

Abgrenzung zwischen Cyber- und physischer Sicherheit (ErwGr 55): In Erwägungsgrund 55 KI-VO ist erläutert, dass Komponenten, die für die ausschließliche Verwendung zu Zwecken der

Cybersicherheit vorgesehen sind, nicht als Sicherheitsbauteile gelten. Die Unterscheidung zwischen Cybersicherheit und physischer Sicherheit ist jedoch nicht in jedem Fall trennscharf möglich. Oftmals haben Cyberangriffe direkte physische (Sicherheits-)Auswirkungen. An dieser Stelle sollte genauer beschrieben werden was unter „die ausschließliche Verwendung zu Zwecken der Cybersicherheit“ fällt. Auch ist es notwendig, die Frage der Erheblichkeit einer Störung im Sinne von Erwägungsgrund 55 näher zu bestimmen.

Klarheit zu Anbieter- vs. Betreiber-Rolle und „wesentlichen Änderungen“ (Art. 25): Unklar ist derzeit noch, in welchen Fällen man nach Art. 25 Abs. 1 KI-VO im Falle von GPAI-Systemen von der Betreiber- in die Anbieterrolle wechselt, da die Kritikalität von GPAI-Systemen vom jeweiligen Anwendungsfall abhängt und sich oftmals nicht von vornherein bestimmen lässt. Wichtig ist in diesem Zusammenhang auch eine Bewertung, wie der grundsätzliche Einsatz von GPAI im Bereich der Personalabteilung einzustufen ist. Geklärt werden sollte beispielsweise: Wird ein Betreiber, der ein GPAI-System mit begrenztem Risiko konzernweit einsetzt durch Art. 25 Abs. 1 lit. c KI-VO zum Anbieter eines Hochrisiko-KI-Systems, wenn er das System (auch) den Mitarbeitenden der Personalabteilung zur Verfügung stellt? Und wenn ja, welche Maßnahmen würden diese Konsequenz vermeiden können?

Viele Begriffe wie z.B. die Definitionen von KI, Hochrisiko-KI, verbotene KI und den daraus resultierenden Maßnahmen des AI Acts sind weiterhin uneindeutig und warten auf Konkretisierung und Standardisierung. Erste vorliegende Leitfäden zur Konkretisierung wie auch die vorgeschlagenen Normen sind jedoch sehr umfassend und erhöhen den bürokratischen Aufwand für Unternehmen.

Wenn es keine klare Abgrenzung in der Definition von KI-Systemen gibt, werden letztendlich die nationalen Gerichte die Kriterien auslegen. Dies wird erneut zu einem nationalen Flickenteppich führen, genau wie bei der Definition von personenbezogenen Daten im Rahmen der DSGVO. Die Leitlinien hätten als Gelegenheit dienen können, diese Definition zu verfeinern und Klarheit zu schaffen, was die Unternehmen bei ihren Umsetzungsbemühungen erheblich unterstützt hätte. Leider wurde diese Chance weitgehend verpasst. Der hilfreichste Aspekt der aktuellen Leitlinien ist die Negativliste, die umreißt, was nicht als KI-System gilt. Die negativen Beispiele sind jedoch nicht sehr detailliert. Die Leitlinien sollten dringend überarbeitet werden, um detailliertere Beispiele und praktische Szenarien aufzunehmen.

Ein konkretes Beispiel für unsichere Einordnungen wäre ein Sicherheitstool, das Anomalien erkennen und entsprechende Maßnahmen ergreifen soll. Die Software erfasst Eingaben wie Netzwerkverkehr, Systemprotokolle und Bedrohungsinformationen und kann automatisch Maßnahmen auslösen (z. B. Blockieren des Datenverkehrs oder Isolieren von Endpunkten), ohne dass ein Mensch in Echtzeit eingreifen muss. Der Grad der Autonomie ist zwar konfigurierbar, aber das System ist von Grund auf für einen (halb-)autonomen Betrieb ausgelegt. Die Software verwendet Algorithmen und maschinelle Lernverfahren, um Ergebnisse wie Anomalieerkennung, Bedrohungsklassifizierung, Risikovorhersage und empfohlene Gegenmaßnahmen abzuleiten.

Die aktuelle Fassung der Leitlinien enthält keine konkreten Beispiele für solche Grenzfälle, was erhebliche Rechtsunsicherheit mit sich bringt. Die Aufnahme weiterer praktischer Beispiele würde Unternehmen dabei helfen, zu bestimmen, ob und wann ihre Systeme oder die von ihnen genutzten Systeme in den Anwendungsbereich des AI Acts fallen.

Außerdem fehlt eine klare Auslegung des vorgesehenen Grandfathering bzw. des Bestandsschutzes für bereits in Verkehr oder in Betrieb genommene Hochrisiko-KI-Systeme basierend auf Art.111 Abs. 2 des AI Acts. Hier ist zu klären, was als wesentliche Konzeptionsänderung verstanden wird, die den festgelegten Bestandsschutz auflöst.

Unternehmen, die KI in ihre Produkte einbauen und dem Kunden zur Nutzung zur Verfügung stellen, sollten nur als "Händler" eingestuft werden; Anwender (Betreiber) sollten nicht zum Anbieter werden. Beispiele aus der Unternehmerschaft zeigen, wie uneindeutig dies oft sein kann: Im Falle einzelner KI-Features von Software für Kunden, im Falle simpler KI-Chatbots, die externes Wissen einbinden, im Falle interner KI-Nutzung mit „Retrieval Augmented Generation“.

Begleitende Maßnahmen zum AI Act: Innovation, Kooperation

Neben dem AI Act sollten weitere Maßnahmen zur Innovationsförderung stehen. Die vorgesehenen Maßnahmen des AI Continent Action Plans, bspw. die Apply AI Strategie, müssen zielführend ausgestaltet und schnell wirksam werden sowie für die Wirtschaft niedrigschwellig nutzbar sein.

Innovationsmaßnahmen sollten zudem viel mehr als bisher auf die Kooperation zwischen den EU-Mitgliedsstaaten wie auch mit vertrauenswürdigen internationalen Partnern setzen, um ausreichend Wirkung entfalten zu können. So sollten z.B. Reallabore oder KI-Fabriken durch mehrere EU-Länder gemeinsam aufgebaut werden, um Standards und Nutzung in einem funktionierenden digitalen Binnenmarkt sicherzustellen.

Harmonisierung von Regeln

Die in den letzten Jahren entstandenen Digitalgesetze der EU sind nicht ausreichend aufeinander abgestimmt. Unterschiedliche Zielrichtungen sowie Lücken und Überlappungen führen zu rechtlichen Unsicherheiten bei Unternehmen. Darüber hinaus sind diverse Begriffe und Maßnahmen in den verschiedenen Regulierungen ähnlich, aber nicht einheitlich und generieren damit Doppelarbeit bei Unternehmen. Hier gilt es schnell Klarheit zu schaffen und die Verpflichtungen aus den verschiedenen Regulierungen effizienter ineinandergreifen zu lassen:

- Automatisierte Entscheidungen: Art. 22 Abs. 2 DSGVO eröffnet Gestaltungsmöglichkeiten für allgemeine wie sektorspezifische Ausnahmen auf EU- wie auf nationaler Ebene für automatisierte Entscheidungen. Diese Möglichkeiten sollten umfassend ausgeschöpft werden.
- Maßnahmen modular angleichen: Die DSGVO und der AI Act fordern z.B. für teilweise überlappende Situationen ähnliche Maßnahmen. Um erheblichen Aufwand zu

reduzieren, sollen diese möglichst deckungsgleich und modular integrierbar gestaltet werden. Dies gilt z.B. für die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und die Risikoabschätzung bei Hochrisikoanwendungen des AI Acts oder für die Anforderungen zur IT-Sicherheit in Art. 32 DSGVO und Art. 15 AI Act.

- Unterschiedliche Verantwortlichkeiten: Zwischen KI-Anbietern (AI Act) und Betreibern (DSGVO) sollten mit Blick auf Haftungspflichten Verantwortlichkeiten eindeutiger abgestimmt werden.
- Ganzheitliche Risikoanalyse: Der Digital Service Act (DSA) erfordert ebenso wie der AI Act Risikoanalysen. Bei gleichzeitigem Anwendungsbereich beider Verordnungen sollten die Möglichkeiten einer ganzheitlichen Risikoanalyse geprüft werden, um auf einmal Anforderungen des AI Acts sowie des DSAs abzudecken.
- Nationale Verzahnung: Ohne Gold-Plating sollen auf nationaler Ebene die Durchführungsgesetze zu den EU-Digitalakten (AI Act, Data Act, DSA…) verknüpft werden, um Synergieeffekte und eine deutliche Arbeitserleichterung für Unternehmen zu schaffen.

Meldepflichten des AI Acts sollten besser auf bestehende Anforderungen abgestimmt werden. Eine einzige, einheitliche Meldeplattform würde einen entscheidenden Unterschied machen – Unternehmen könnten Vorfälle nur einmal melden, anstatt ihre Bemühungen über mehrere Rahmenwerke hinweg zu duplizieren.

Wichtig ist in diesem Zusammenhang auch, sektorale Regulierung und den AI Act besser zu verzahnen. Der AI Act als horizontale Regulierung gilt auch für KI-Systeme in Bereichen, die bereits durch sektorale Regulierung auf klassische Gefahren z.B. auf Gesundheit und Sicherheit eingehen. Dabei bestehen sektorspezifische Regeln und der AI Act mit ähnlichen aber oft nicht gleichen Anforderungen nebeneinander und führen zu unnötigen Doppelarbeiten und Unklarheiten. So ist bspw. Art. 10 des AI Acts weitgehend identisch mit Art. 174 der Capital Requirements Regulation (CRR), jedoch legt keine Normung da, welche Elemente von Art. 10 als durch Art. 174 CRR abgedeckt gelten sollen. Eine Harmonisierung und Klärung des Zusammenspiels sektoraler Regulierungen mit dem Act ist dringend erforderlich. Hierfür können unterschiedliche Ansätze aufgegriffen werden:

- Lex Specialis präzisieren: Im Falle eines Konflikts zwischen EU-Rechtsvorschriften soll die Empfehlung aus dem Draghi Competitiveness Report umgesetzt werden, wonach die sektorale / spezifischere Vorschrift automatisch Vorrang hätte.
- Konkrete Ausweisung Lead Act: Damit würde die Einhaltung der sektoralen Regulierung, z.B. die Medizinprodukteverordnung (MDR), auch alle Anforderungen aus dem AI Act automatisch mit umfassen. Wo nötig können einzelne Vorgaben aus dem AI Act, die signifikant über die sektorale Regulierung hinausgehen, explizit als verpflichtend benannt werden. Das kann das AI Office mit einer Durchführungsverordnung direkt umsetzen.
- Konkrete Ausweisung einzelner Anforderungen: In Art. 17 Abs. 4 des AI Acts wird klar geregelt, welche Ansprüche des AI Acts durch die Einhaltung des

Finanzdienstleistungsrechts abgedeckt sind und welche zusätzlichen Anforderungen aus dem AI Act noch zu erfüllen sind. Eine solche Regelung braucht es für alle betreffenden sektoralen Regelungen und überlappenden Anforderungen.

- KI in sektorale Regulierung integrieren: Alternativ könnten KI-Themen in sektorale Regulierungen integriert werden. Ein zentraler Koordinator sollte dazu die Einheitlichkeit der KI-Behandlung zum AI Act sicherstellen.

Daten und Datenschutz

Daten sind ein wesentlicher Bestandteil und bieten die Grundlage für eine Vielzahl von Anwendungen, darunter auch Künstliche Intelligenz. Daher ist es elementar, den Zugang zu Daten für die Unternehmen so unkompliziert wie möglich zu gestalten.

Nicht kohärente, komplexe und rechtsunklare Regelungen bei den datenbezogenen Verordnungen sind insb. herausfordernd für kleinere und Midcap-Unternehmen mit starken datengetriebenen Geschäftsmodellen und Innovation werden so eher gehemmt als gefördert. Vorschriften der DSGVO und der Datenökonomie (insb. Data Act, Digital Markets Act, Digital Services Act, AI-Act) sollten konsistent und kohärent zueinander gestaltet und damit mehr Rechtssicherheit geschaffen werden.

Eine Kohärenz sollte auch herbeigeführt werden für alle Stufen der Datenverarbeitung mit KI sowie für eine rechtssichere Nutzung von Datenräumen.

Geplante EU-Datenunion

Die strategische Zielsetzung, mit der Data Union Strategy einen kohärenten und wettbewerbsfähigen europäischen Datenbinnenmarkt zu schaffen, ist grundsätzlich zu begrüßen. Auch die ersten Überlegungen möglicher konkreter Ansätze, vermehrte Investitionen in Technologien und Datenverfügbarkeit sowie die Vereinfachung und Konsolidierung bestehender regulatorischer Richtlinien werden positiv bewertet.

Gleichzeitig können die geplanten Maßnahmen nur dann ihre Wirkung entfalten, wenn sie für Unternehmen niedrigschwellig nutzbar sind. Der wichtigste Hebel für Unternehmen bei der Nutzung von Daten bzw. der Entwicklung von KI ist ein klarer und handhabbarer sowie innovationsfreundlicher regulatorischer Rahmen.

Während ein funktionierender Datenbinnenmarkt ein wesentlicher Treiber für Innovation und Wachstum sein kann, darf der Schutz sensibler Daten – insbesondere Daten kritischer Infrastrukturen – nicht vernachlässigt werden. Daten sicherheitsrelevanter Bereiche erfordern einen besonders hohen Schutz und dürfen keinesfalls unkontrolliert geteilt werden. Eine übermäßige Vereinfachung der einschlägigen Regeln könnte in diesem Bereich mehr Schaden als Nutzen anrichten. Ein ausgewogener Ansatz, der sowohl wirtschaftliche Potenziale als auch sicherheitsrelevante Aspekte berücksichtigt, ist daher unverzichtbar, um die strategischen Ziele der

Datenunion erfolgreich umzusetzen. Aber auch außerhalb des sicherheitsrelevanten Bereichs ist darauf zu achten, dass Daten in Unternehmen häufig das Ergebnis von Investition und Innovation sind, die daher als wirtschaftliches Eigentum und als Geschäftsgeheimnis schützenswert sein können. Bei jeder Überlegung zu einer Datenteilungspflicht sind daher die Interessen derjenigen Unternehmen, die die Daten generiert haben, mit den Interessen derjenigen Unternehmen, die fremde Daten nutzen wollen, angemessen abzuwägen. Ggf. kann – je nach wirtschaftlichem Vorteil für das datenempfangende Unternehmen und nach dem „Wert" der Daten für das datenabgebende Unternehmen – auch ein (finanzieller) Ausgleich für die Datenabgabe sinnvoll sein.

Data Governance Act

Der Data Governance Act zielt darauf ab, den Datenaustausch zwischen Unternehmen, Einzelpersonen und öffentlichen Stellen innerhalb der EU zu erleichtern und zu fördern, um die Verfügbarkeit von Daten zu erhöhen. Das soll dann über sogenannte Datenvermittlungsdienste ablaufen. Um Daten für Wirtschaft, Forschung, Innovation und Umweltschutz nutzen zu können, soll das freiwillige Zurverfügungstellen von Daten – der Datenaltruismus – gefördert werden. Um als datenaltruistische Organisation anerkannt zu werden, müssen Einrichtungen bestimmte Anforderungen erfüllen und ein Anerkennungsverfahren durchlaufen. Zur Förderung breiten Datenaustausches sollten diese Anforderungen und Verfahren vereinfacht werden, um Unternehmen nicht von solch sinnvollen Mechanismen abzuschrecken.

Unternehmen können gleichzeitig sowohl Anbieter eines Datenvermittlungsdienstes (Art. 2 Abs. 11 und Art 10 ff. DGA), eine datenaltruistische Organisation (Art. 2 Abs 16, Art. 16 DGA) als auch Betreiber eines Datenraumes unter Art. 33 Data Act sein. Auch möglich ist, dass der Datenraum unter Art. 33 oder ein beinhaltetes System darin als Datenverarbeitungsdienst (Art. 2 Abs. 8 DA) gilt. In Summe sind unter Umständen vier Konzepte auf das gleiche Unternehmen anwendbar, ohne dass das Verhältnis zwischen diesen erklärt oder strukturiert wird.

Das Zusammenspiel zwischen Art. 12 (j) DGA, bzw. die Festlegung, dass der Anbieter eines Datenvermittlungsdienstes bestimmte Maßnahmen ergreifen muss, um rechtswidrige Transfers von nicht-personenbezogene Daten in Drittstaaten zu vermeiden und dem Fall, dass ein Datenvermittlungsdienst als Datenverarbeitungsdienst gem. Data Act gilt und Art. 32 DA anwendbar ist, ist weder erklärt noch strukturiert. Hier sollte ein Verweis die technischer organisatorischen Maßnahmen klären.

Es ist unklar, wie Art. 12 (j) des DGA mit der DSGVO harmonisiert. Bei einer parallelen Verarbeitung von personen- als auch nicht-personenbezogenen Daten in einem nicht-trennbaren Set führt dies zu Problemen. Es braucht klare, rechtsverbindliche Vorgaben zu Pseudonymisierung und Anonymisierung, um eine Rechtssicherheit bei der Verarbeitung gemischter Datensätze zu gewährleisten.

Data Act

Grundsätzlich ist zu überdenken, inwieweit sichergestellt werden kann, dass europäische Unternehmen im internationalen Wettbewerb nicht gegenüber global aktiven Unternehmen durch das verpflichtende Datenteilen benachteiligt werden.

Relevante Begriffe wie „Dateninhaber“ und „Nutzer“ müssen zwingend weiter konkretisiert werden, um die Umsetzung des Data Acts zu erleichtern. Insbesondere bei der Definition von „Nutzer“ ergeben sich derzeit in Konstellationen mit mittelbaren Besitzverhältnissen sowie in längeren Besitz- und Wertschöpfungsketten Unklarheiten bei der Identifizierung.

Auch der Begriff „Data Processing Services“ benötigt eine klare Differenzierung. Nach aktueller Definition kann er IaaS, PaaS und SaaS umfassen – drei grundsätzlich unterschiedliche Servicemodelle.

Im Zusammenspiel von Data Act und DSGVO ist Folgendes zu beachten: Der Data Act sieht zwar vor, dass die DSGVO unberührt bleibt und deren Regelungen bei personenbezogenen Daten (Artikel 1(5)) weiterhin uneingeschränkt gelten. Dennoch bestehen ungeklärte Fragen zu Verantwortlichkeiten und Meldepflichten im Spannungsfeld der beiden Verordnungen, die derzeit ein erhebliches Risiko für Unternehmen darstellen.

Grundsätzlich besteht ein Spannungsfeld zwischen dem „Privacy-by-Design“ Grundsatz der DSGVO (Art. 25 DSGVO) und den darauf basierenden strengen Anforderungen der Verarbeitung von personenbezogenen Daten und dem „Access-by-Design“ Prinzip des Data Acts.

Auch offen ist, wie Unternehmen mit Mischdatensätzen umgehen sollen, denn der Data Act enthält keine Rechtsgrundlage für die Verarbeitung. Denkbar wäre die Einführung einer Rechtsgrundlage im Data Act nach der DSGVO für die Verarbeitung personenbezogener Daten, bzw. Art. 4(1) und Art. 5(1) des Data Acts als mögliche Grundlage nach Art. 6(1) DSGVO, Daten zu verarbeiten.

Eine Harmonisierung bzw. eindeutige Klärung hinsichtlich der Abgrenzung zwischen personenbezogenen und IoT-Daten ist zwingend erforderlich. Ebenso muss präzise festgelegt werden, unter welchen Bedingungen personenbezogene Daten sicher als anonymisiert gelten. Hierbei braucht es eindeutige Kriterien sowie technische Standards, an die sich Unternehmen halten können.

Harmonisierungsbedarf besteht auch 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. Es ist unklar, inwieweit die beiden Regelungsbereiche jeweils operationalisiert werden müssen bzw. sollten diese möglichst deckungsgleich gestaltet werden.

Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DSGVO) ist für viele Unternehmen auch heute noch ein großes Thema, mit dem zahlreiche Umsetzungsschwierigkeiten und weitere Herausforderungen einhergehen. Grundsätzlich ist eine Reduktion des bürokratischen Aufwands wichtig: Proportionalität basierend auf dem Risikoniveau und Reduzierung der fragmentierten Aufsicht. Die DSGVO sollte der Entwicklung innovativer Technologien nicht im Wege stehen und muss einen stabilen Rechtsrahmen bilden. Aufgrund des hohen Abstraktionsgrades mit der Vielzahl an sog. Unbestimmten Rechtsbegriffen, welche der Auslegung im Einzelfall bedürfen, erfüllt die DSGVO diese Anforderung nicht.

Strittige/offene Auslegungsfragen zu wesentlichen Aspekten der DSGVO, bspw. Art 6 Abs 1 lit. f müssen zumindest in den Erwägungsgründen klargestellt werden. Ferner müssen die Vorschriften der DSGVO und der Datenökonomie konsistent und kohärent zueinander gestaltet werden. Dies beinhaltet auch die Schaffung von Rechtsgrundlagen für alle Stufen der Datenverarbeitung mit KI sowie für eine rechtssichere Nutzung von Datenräumen. Auch für private Wissenschaftsunternehmen sollten solide Rechtsgrundlagen geschaffen werden, damit diese gemeinsam mit öffentlichen Wissenschaftseinrichtungen Forschung vorantreiben können (z. B. über eine Erweiterung des Art. 5 Abs. 1 lit. b) HS 2 (Alt.2) DSGVO oder spezialgesetzlich).

Für datengetriebene Prozesse (z. B. Big Data, KI, Blockchain) hat sich gezeigt, dass Unternehmen hier bei den Rechtsgrundsätzen "Transparenz", "Zweckbindung", "Datenminimierung" und "Speicherbegrenzung" an Grenzen von Auslegung und rechtlichen Möglichkeiten stoßen. Als die Digitalisierung begleitendes Recht müsste überlegt werden, wie über die DSGVO - z. B. durch Auslegung von Rechtsgrundlagen wie Art. 6 Abs. 1 lit. f bzw. Art. 6 Abs. 4 DSGVO oder auf sonstige Weise -den Unternehmen mehr Rechtssicherheit in diesen wichtigen Fragen gegeben werden kann.

Nicht zuletzt sollte im Zuge einer Vereinfachung die Zusammenarbeit unter den europäischen Datenschutzaufsichtsbehörden und die Streitbeilegung effizienter gestaltet werden. Insbesondere sollte frühzeitig ein Konsens zwischen den Datenschutzbehörden herbeigeführt werden können, um so die Rechtssicherheit bei der Umsetzung der DSGVO EU-weit zu fördern.

Weitere Themen und Berichtspflichten

Insbesondere das Thema „Datenein- und Weitergabe“ kann bei kleinen Unternehmen zu viel Ressourcenaufwand führen. Wichtig ist es, Once Only Prinzipien konsequent einzuführen. Beispielsweise müssen im Bereich der Energieversorgung und PV-Anlagen Kundendaten oft noch manuell und mehrfach an Energieversorgungsunternehmen übermittelt werden, mit uneinheitlichen Schnittstellen und Interfaces. Insbesondere staatliche Webinterfaces sollten vereinheitlicht werden, die doppelte Eingabe sensibler Daten sollte vermieden werden.

Cookies und Tracking

Teilweise werden bestehende Regelungen als veraltet und hinderlich wahrgenommen und eine Re-Evaluierung der bestehenden Cookie- und Tracking-Regularien wird begrüßt. Vereinzelt wird sogar eine ePrivacy VO begrüßt. Anderseits werden bestehende Regelungen – insbesondere vor dem Hintergrund des § 25 TDDDG – als ausreichend empfunden und in einer weiteren Richtlinie eher die Gefahr der Über- bzw. vermeidbaren Doppelregulierung gesehen.

Sollte eine neue Richtlinie umgesetzt werden, so kommt es darauf an, dass diese dazu beiträgt, klare Vorgaben und Standards für die Verwendung von Cookies und Tracking zu etablieren und dadurch den Aufwand für Webseitenbetreiber zu reduzieren.

ePrivacy

Die Vereinheitlichung und Harmonisierung der ePrivacy Richtlinie als Verordnung wäre grundsätzlich immer noch zu begrüßen, denn eine Vereinheitlichung der Gesetzesauslegung ist für Unternehmen von großem Vorteil. Konkretisierungen sollten dabei direkt in den Erwägungsgründen enthalten sein, um für Rechtsklarheit zu sorgen.

Informations- und Dokumentationspflichten müssen immer verhältnismäßig sein. Neue rechtliche Rahmenbedingungen müssen sachgemäß sein. Anpassungen von Websites, Apps oder IoT verursachen hohen personellen wie finanziellen Aufwand. Diese ziehen zudem eine Anpassung von Datenschutzdokumentationen nach sich. Der Staat darf die Unternehmen nicht mit Kosten, Pflichten und laufenden neuen Anpassungen überfordern. Verpflichtend zu implementierende technische Schutzmaßnahmen müssen zwingend einwilligungsfrei sein. Apps oder IoT verursachen hohen personellen wie finanziellen Aufwand. Diese ziehen zudem eine Anpassung von Datenschutzdokumentationen nach sich. Der Staat darf die Unternehmen nicht mit Kosten, Pflichten und laufenden neuen Anpassungen überfordern. Verpflichtend zu implementierende technische Schutzmaßnahmen müssen zwingend einwilligungsfrei sein.

Digital Services Act

Bezogen auf den Digital Services Act (DSA) stellt insbesondere Art. 20 eine Belastung für die Unternehmen dar. Die Vorgabe zur Implementierung des Beschwerdeprozesses hängt an der Klassifizierung einer Plattform als Marktplatz, unabhängig davon, ob auf der Plattform Nutzer eigene Inhalte (user generated content, UGC) pflegen können. Dies führt bei Geschäftsmodellen, die ohne UGC auskommen, zu unnötigen Belastungen, da auch diese Unternehmen Beschwerdeprozesse implementieren müssen.

Digitale Identität und Business Wallet

Digitale Identitäten als eines der Themen aus dem Sondierungsdokument sind unter anderem für die Kommunikation von Unternehmen mit der öffentlichen Verwaltung vielfach von Relevanz.

Digitale Identität

Hinsichtlich der digitalen Identität bleibt in der Initiative offen, welcher Aufwand hiermit für Betreiber von Websites verbunden wäre. Der Betreiber der Website müsste den Online-Ausweis der Nutzer über verschiedene Ident-Verfahren einbinden und selbst den elektronischen Identitätsnachweis erbringen oder einen externen Identifizierungsdiensteanbieter die Authentifizierung (sowie bei Bedarf die Identifizierung) der Nutzenden übernehmen lassen. Vor allem Unternehmen aus regulierten Branchen wie dem Finanz- oder Telekommunikationssektor werden wohl dazu verpflichtet sein, die EU-Wallet ab ihrem Vorhandensein für digitale Identitätsprüfungen zu akzeptieren. Dies erfordert die Schaffung geeigneter Schnittstellen sowie eine Anpassung der internen Abläufe. Vorteile für Unternehmen könnten in einer effizienteren Kundenidentifikation, der Automatisierung von Prozessen zur Identitätsprüfung (KYC – Know Your Customer) und gegen Geldwäsche (AML – Anti-Money Laundering) liegen. Der technische sowie finanzielle Aufwand für Websitebetreiber – insbesondere KMU - muss mitgedacht und in Grenzen gehalten werden.

Insbesondere sind Herausforderungen in Bezug auf Datenschutz und die Integration in bestehende IT-Systeme zu erwarten, die vor einer weiteren Regulierung und Inbetriebnahme der Wallet zwingend gelöst sein sollten und die Unternehmen nicht vor neue Rechtsunsicherheit stellen dürfen.

EU Business Wallet

Die EU Business Wallet (EUBW) kann insbesondere für KMU ein wichtiges sowie effektives Mittel der Zukunft sein, um digitale Prozesse sicher umzusetzen sowie grenzüberschreitende Geschäftsprozesse und Interaktion mit Behörden zu gestalten. Damit das Potenzial der EUBW umfangreich ausgeschöpft werden kann, sollten bei der Umsetzung schon jetzt die folgenden Punkte berücksichtigt werden:

Wichtig ist, dass alle wirtschaftlichen Akteure – darunter auch Selbstständige - von der EUBW profitieren können. Da die überwiegende Mehrheit der Unternehmen auf Vertreter wie Steuerberater oder Rechtsanwälte vertraut, sollten die Vertretungsbefugnisse und Vollmachten im Konzept der EUBW entsprechend berücksichtigt werden. Zudem sollte dabei – insbesondere auf geringe Kosten, zeiteffiziente Verfahren und die Bereitstellung gezielter Unterstützungsmaßnahmen geachtet werden. Weiterhin wichtig ist eine interoperable Gestaltung über mitgliedstaatliche Grenzen hinweg und die Möglichkeit, auch Nachrichten zu versenden. Nicht zuletzt sollte auf Technologieoffenheit und Vermeidung von Parallelstrukturen geachtet werden.

Nur wenn die Umsetzung konsequent durch alle Mitgliedstaaten erfolgt und als Ergebnis eine Wallet vorliegt, die unternehmensfreundlich sowie praxistauglich ist, können sich die Potentiale vollständig zeigen. Eine frühzeitige Einbindung relevanter Stakeholder – darunter insbesondere Unternehmen und deren Interessenvertreter - könnte dazu beitragen, die Herausforderungen zu meistern und mit der Wallet einen echten Mehrwert für Unternehmen zu schaffen.

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

Arian Siefert
Referatsleiter Wirtschaft digital
Tel: +49 30 20308 2118 / Mobil: +49 151 1131 3039
E-Mail siefert.arian@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.

Vertretung der DIHK | Deutsche Industrie- und Handelskammer bei der EU
19 A-D, Avenue des Arts | B-1000 Bruxelles
Tel. +32 2 286-1611 | Fax +32 2 286-1605 | Internet: www.dihk.de