Digitalgesetz-gebung der EU: Konfliktzonen und Wege zur Kohärenz

Version 1.0 – April 2025

bitkom

Digitalgesetzgebung der EU: Konfliktzonen und Wege zur Kohärenz

Version 1.0 – April 2025

Das Papier zeigt zentrale Herausforderungen, die durch die vielfältigen Digitalrechtsakte auf europäischer Ebene entstehen auf. Während DS-GVO, Data Act, AI Act, DSA oder DMA jeweils eigene Schwerpunkte setzen, führen Überschneidungen, Doppelregelungen und uneinheitliche Begriffsdefinitionen zunehmend zu Rechtsunsicherheit und erhöhtem Verwaltungsaufwand.

Die in diesem Papier dargestellte Übersicht beleuchtet konkrete Konfliktfelder, mögliche Spannungsbereiche und zeigt erste Lösungsansätze auf, um Widersprüche in den bestehenden und geplanten Regelungen zu minimieren. An einigen Stellen werden zudem Probleme innerhalb eines Rechtsaktes aufgezeigt. Das Papier soll laufend aktualisiert werden.

Inhalt

1 Allgemein

Rechtsakt	Problem	Mögliche Lösung
Rechtsakt-übergreifend	**Symptom- statt Ursachenbekämpfung:** Generelles Problem der uneinheitlichen Definitionen bzw. unterschiedlichen Verständnissen von Rechtsbegriffen. Bspw. »Dark Patterns« – das Verbot von Dark Patterns findet sich im Data Act (EwG 38), dem DSA (Art. 25) und dem DMA (Art. 6 Abs. 3 EwG 50ff.) Dennoch wird der Begriff wieder in der Vorbereitung des Digital Fairness Acts verwendet, während noch nicht klar ist, was damit gemeint ist bzw. keine Einigkeit über die Definition besteht.	Orientierung an Definition in Art. 25 DSA inkl. der Regelbeispiele und Leitlinien nach Art. 25 Abs. 3 DSA
Rechtsakt-übergreifend	**Problem von Unberührt-Regelungen:** Unberührt-Regelungen helfen nicht zur Auflösung von Zielkonflikten der verschiedenen digitalen EU-Rechtakten. Art. 2 Abs. 7 AI Act, Art. 2 Abs. 4 g) DSA und EwG 7 Data Act besagen z.B., dass die DS-GVO unberührt bleibt. Dennoch beeinflussen und überschneiden sich die EU-Rechtsakte in vielen Bereichen der praktischen Umsetzung.	Konkrete Vorrangregelungen Harmonisierte Begriffserklärungen (einheitliche Definitionen) Gemeinsame Praxishandreichungen und Leitfäden durch bspw. die Kommission, die gezielt typische Konfliktszenarien in der praktischen Umsetzung beschreiben und Lösungen liefern

2 Zwischen DS-GVO und ...

Rechtsakt	Problem	Mögliche Lösung
Data Act	**Datenzugriffsrechte im Data Act vs. Betroffenenrechte der DS-GVO:** Die im Data Act verankerten Zugriffsrechte (Art. 3-5 DA) stehen potenziell in Konflikt mit den Betroffenenrechten der DS-GVO, wie dem Recht auf Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten (Art. 16 ff. DS-GVO). Dies kann dazu führen, dass bei der Offenlegung von Daten im Rahmen des Data Act unbeabsichtigt Persönlichkeitsrechte beeinträchtigt werden.	Durch den Einsatz von Pseudonymisierungs- oder Anonymisierungsverfahren kann gewährleistet werden, dass bei der Datenweitergabe keine direkt identifizierbaren personenbezogenen Informationen offengelegt werden. Jedoch ist zu beachten, dass der Einsatz pseudonymer Daten beim DA nicht hilft. Vorschlag daher: gemischte Datensätze werden nicht wie pb-Daten behandelt, wenn die pb-Daten nach anerkannten Standards pseudonymisiert sind und eine Repersonalisierung durch unbefugte Dritte ausgeschlossen ist. Solche Maßnahmen erlauben den Zugang zu den für den Data Act relevanten Daten, ohne die DS-GVO-Bestimmungen zu verletzen. In Fällen, in denen beide Rechtsakte anwendbar sind, sollte geprüft werden, ob die spezifischeren Regelungen des Data Act Vorrang haben – sofern dies mit dem Schutz der Betroffenenrechte vereinbar ist.
Data Act	**Rechtsgrundlage der DS-GVO bei divergierenden Rollen von Nutzern und Betroffenen im Data Act:** Auf welche Rechtsgrundlage der DS-GVO greift man zurück, wenn Nutzer nach Data Act und Betroffener nach DS-GVO auseinanderfallen?	Siehe grds. Erwägungsgründe 7 und 34 DA. Die Lösung könnte eine Klarstellung im Verordnungstext selbst statt in den Erwägungsgründen sein.
Data Act	Sieht der Data Act die Möglichkeit der Auftragsverarbeitung im Sinne der DS-GVO auch für einen Datenempfänger vor, oder müssen diese die Daten stets selbst verarbeiten: Kann ein Datenempfänger Daten im Sinne einer Shared Data Economy bei Einwilligung des Nutzers durch einen Auftragsverarbeiter verarbeiten lassen?	Der Gesetzgeber sollte explizit bestimmen, unter welchen Umständen die DS-GVO-Grundlagen herangezogen werden und wie im Falle divergierender Definitionen vorzugehen ist. Eine systematische Abgrenzung – etwa über spezifische Anwendungsfälle oder Datenkategorien – kann hier als Leitfaden dienen.
Data Act	**Risikopotenzial durch Datenklassifizierung im Data Act:** Die Pflicht zur Differenzierung zwischen personenbezogenen und nicht-personenbezogenen Daten und Geschäftsgeheimnissen birgt für Dateninhaber ein erhebliches Risikopotenzial. Unklare oder fehlerhafte	Die Einführung standardisierter, technischer Verfahren zur automatisierten Klassifikation von Daten unterstützt Dateninhaber dabei, ihre Daten korrekt zu kategorisieren.

Rechtsakt	Problem	Mögliche Lösung
	Klassifizierungen können zu Haftungsfragen, Wettbewerbsnachteilen und unsicheren Rechtsfolgen führen, wenn beispielsweise versehentlich personenbezogene Daten unzureichend geschützt weitergegeben werden.	Zertifizierungsprogramme für Datenmanagementsysteme können als Nachweis der Einhaltung dieser Standards dienen und das Vertrauen in die angewandten Verfahren stärken.
Data Act	**Umgehung des Data Act durch Vermischung von Daten:** Unternehmen, die kein Interesse an der Datenweitergabe haben, könnten versucht sein, generierte Daten mit personenbezogenen Daten zu vermengen, um so den Anwendungsbereich des Data Acts zu umgehen. Dadurch würde die beabsichtigte Transparenz und der Zugang zu Daten unterlaufen, während gleichzeitig der Schutz personenbezogener Daten oberhalb der DS-GVO-Regeln gewährleistet bleibt.	Option 1: Klare, rechtsverbindliche Vorgaben zu Pseudonymisierung und Anonymisierung verfügbar machen. Option 2: Recht auf Datenzugang im Zweifel höher gewichten, wenn pb-Daten nach anerkannten Standards pseudonymisiert sind Anerkennung von Code of Conducts zu Pseudonymisierung, gemeinsames Verständnis von Aufsichtsbehörden, Guidelines der Kommission. Da pseudonymisierte Daten momentan aber als personenbezogene Daten betrachtet werden, kommt nur eine Anonymisierung in Betracht.
Data Act	**Abgrenzung von DS-GVO-Auskunftsanspruch und Data Act-Datenzugangsrecht:** Der Auskunftsanspruch gemäß Art. 15 DS-GVO zielt primär darauf ab, betroffenen Personen Einsicht in die zu ihrer Person gespeicherten Daten zu gewähren. Das Datenzugangsrecht aus dem Data Act hingegen soll einen standardisierten und breit angelegten Zugang zu Daten ermöglichen – und das auch für personenbezogene Daten. Daraus ergibt sich die Frage, welchen konkreten Vorteil ein solches Datenzugangsrecht im Vergleich zum traditionellen DS-GVO-Auskunftsanspruch bietet.	Rolle des einzelnen Nutzers im Kontext der Freigabe von Daten kritisch hinterfragen. Möglicherweise wäre die Vertragserfordernis ausreichend für die Weitergabe von Daten und es benötigt keine proaktive Beantragung einer Auskunft seitens des Nutzers.
Data Act	**Spannungsverhältnis zwischen DS-GVO-Datenportabilität und Data Act-Zugangsrechten:** Die DS-GVO (z. B. Art. 5, 6 und 7) legt strenge Anforderungen an die Verarbeitung personenbezogener Daten fest. Der Data Act hingegen will den Zugang zu und die Weitergabe von Daten – häufig auch aus vernetzten	Es sollte geprüft werden, inwieweit das bestehende Konzept der Datenportabilität den Anforderungen des Data Act gerecht wird. Eine Anpassung des Art. 20 DS-GVO könnte darin bestehen, den Anwendungsbereich zu erweitern oder differenzierte Schutzmechanismen

Rechtsakt	Problem	Mögliche Lösung
	Geräten – erleichtern. Art. 20 DS-GVO (Recht auf Datenportabilität) muss im Kontext des Data Act, der unter Umständen breiter angelegte Datenzugangsrechte vorsieht, neu ausbalanciert werden.	zu integrieren, die den erweiterten Zugriffsrechten allein im Data Act Rechnung tragen. Eine Überarbeitung und Abstimmung der relevanten Bestimmungen der DS-GVO und des Data Act sollte erfolgen, um eine konsistente Rechtsordnung zu schaffen. Dies umfasst insbesondere die Sicherstellung, dass die erweiterten Datenzugriffsrechte nicht zulasten der betroffenen Personen gehen.
Data Act	**Zielkonflikt zwischen Datenzugang und Datenschutz im Data Act:** Der Data Act fordert mit »Access by Design« eine möglichst einfache und standardisierte Zugänglichkeit zu großen Datenmengen – auch personenbezogener Daten –, um Innovationen und Wettbewerbsfähigkeit zu fördern. Dagegen verlangt die DS-GVO mit »Privacy by Design«, dass der Schutz personenbezogener Daten von Beginn an in Produkte und Prozesse integriert wird. Bei der Produktentwicklung können diese Zielsetzungen in einen Zielkonflikt geraten, da ein uneingeschränkter Datenzugang nicht ohne Risiko für die Privatsphäre der Nutzer realisierbar ist.	Hinweis: Unabhängig von Data Act müssen Produkte und Services die pb-Daten verarbeiten, grundsätzlich die Anforderungen aus Art. 25 und 32 DS-GVO erfüllen. Es wäre paradox, auf diese Anforderungen zu verzichten, je stärker diese Produkte und die verbundenen Services vernetzt sind und damit das Risiko steigt. Im Übrigen müssen Privacy by Design und Access by Design kein Wiederspruch sein, wenn beides von Anfang an zusammen gedacht wird.
AI-Act	**Überschneidungen zwischen VvV und AI-Act-Pflichten:** Art. 30 DS-GVO verpflichtet Unternehmen zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten – ein Nachweis, der Ähnlichkeiten zu den Risikobewertungs- und Post-Market-Monitoring-Pflichten des AI Acts aufweist. Diese Überschneidungen können zu redundanten administrativen Belastungen führen und erschweren eine einheitliche Anwendung der Regularien, insbesondere für Unternehmen, die sowohl personenbezogene Daten verarbeiten als auch KI-Systeme einsetzen.	Entwicklung einheitlicher Leitlinien, die beide Regelwerke – DS-GVO und AI Act – berücksichtigen und einen gemeinsamen Standard für die Dokumentation von Verarbeitungstätigkeiten, Risikobewertungen und Überwachungsprozessen schaffen. Klarstellung, in welchen Fällen erweiterte Nachweise (z. B. Post-Market-Monitoring bei KI-Systemen) zusätzlich zu den Standardanforderungen des Art. 30 DS-GVO erforderlich sind.
AI-Act	**Bedarf nach integrierter Risikobewertung:** Art. 2 (7) AI Act besagt, dass die DS-GVO unberührt bleibt. Dennoch beeinflusst der AI Act in vielen Bereichen die praktische Umsetzung der DS-GVO,	Eine Integration der Risikobewertungen des AI Act (z. B. Grundrechte-Risikoanalysen) in Datenschutz-Folgenabschätzungen nach Art. 35 DS-GVO wird als sinnvoll angesehen, um Doppelarbeit zu vermeiden (s.o).

Rechtsakt	Problem	Mögliche Lösung
	insbesondere bei Interessenabwägungen, Risikobewertungen und Haftungsfragen.	
AI-Act	**Konflikt zwischen Datensparsamkeit und Anti-Bias-Maßnahmen in der KI-Entwicklung:** Ein Spannungsfeld ergibt sich aus dem Grundsatz der Datensparsamkeit und den Anti-Bias-Maßnahmen bei generativer KI oder Nicht-Hochrisiko KI Art. 9 DS-GVO verbietet grundsätzlich die Verarbeitung sensibler Daten (z. B. ethnische Herkunft, Religion, Gesundheit), es sei denn, es liegt eine Ausnahme vor (z. B. öffentliches Interesse). Art. 10 (5) AI Act erlaubt die Verarbeitung sensibler Daten in Hochrisiko-KI-Systemen, um Diskriminierung zu erkennen und zu verringern. Diese Ausnahme gilt jedoch nicht für generative KI oder nicht-Hochrisiko-Systeme, obwohl auch hier Diskriminierungspotenziale bestehen. Die Vorgaben der DS-GVO stehen der notwendigen Verarbeitung sensibler Daten für Bias-Reduktion oft im Weg. Entwickler könnten sich einem hohen Haftungsrisiko aussetzen, wenn sie Daten verwenden, um Diskriminierungen zu bekämpfen.	Erweiterung der bestehenden Ausnahmen für die Verarbeitung sensibler Daten, sodass sie auch auf generative KI oder Nicht-Hochrisiko-Systeme angewendet werden können, sofern dies ausdrücklich dem Zweck der Diskriminierungsvermeidung dient. Dafür müssten klare Schutzmechanismen etabliert werden, etwa strenge Zweckbindung, pseudonymisierte oder anonymisierte Datensätze und verbindliche Risiko- und Folgenabschätzungen, die die Rechte und Freiheiten der betroffenen Personen wahren.
AI-Act	**Spannungsfeld Datenerhebung und Performance:** Es besteht ein Konflikt zwischen den Performanceanforderungen des AI Act (Art. 15) und den Bestimmungen der DS-GVO (Art. 9). Art. 15 Abs. 1 AI Act fordert für Hochrisiko-Systeme ein »angemessenes Maß an Genauigkeit«, wobei Genauigkeit richtigerweise als Performanz bzw. Leistungsfähigkeit i. S. v. technischen Gütemaßen zu lesen ist. Für die Entwicklung leistungsfähiger KI-Modelle, insbesondere im medizinischen Bereich, ist jedoch teilweise die Verarbeitung sensibler Daten notwendig (z. B. Gesundheitsdaten). Die Nutzung solche Daten könnte nach dem AI Act erforderlich sein, um die hinreichende Leistung und auch die Abdeckung diverser Bevölkerungs-gruppen durch das KI-Modell zu gewährleisten. Art. 9 DS-GVO hingegen verbietet die Nutzung bestimmter Kategorien von sensitiven Daten.	Möglich wäre die Schaffung einer engen Ausnahmevorschrift, die es KI-Entwicklern bei Hochrisiko-Anwendungen oder vergleichbar sensiblen Einsatzfeldern explizit erlaubt, sensible Daten nach strengen Auflagen zu verarbeiten, sofern dies für die erforderliche Genauigkeit und Leistungsfähigkeit der Modelle unbedingt notwendig ist. Dabei könnten robuste Schutzmaßnahmen wie Pseudonymisierung, Verschlüsselung, eine klare Zweckbindung und umfassende Risiko- und Folgenabschätzungen vorgeschrieben werden, damit die datenschutzrechtlichen Anforderungen gewahrt bleiben.

Rechtsakt	Problem	Mögliche Lösung
AI-Act	**Wiederverwendung personenbezogener Daten für das Training von KI-Modellen:** Es fehlt eine klare Regelung zur Wiederverwendung personenbezogener Daten für das Training von KI-Modellen. Ob die Nutzung rechtmäßig ist, hängt – insbesondere vor dem Hintergrund des Zweckbindungsgrundsatzes nach Art. 5 Abs. 1 b) DS-GVO – stark vom Einzelfall ab. Die nachträgliche Einholung von Einwilligungen für KI-Training wäre oft nicht praktikabel.	Schaffung einer klaren, einheitlichen Rechtsgrundlage, die es unter bestimmten Voraussetzungen erlaubt, personenbezogene Daten aus bereits erhobenen Datensätzen für das KI-Training zu verwenden, ohne jeweils eine neue Einwilligung einholen zu müssen. Diese Rechtsgrundlage könnte an strenge Bedingungen geknüpft sein, etwa Zweckbindung, Pseudonymisierung, Risikobewertungen und eine Begrenzung der Nutzung auf jene Fälle, in denen sie erforderlich ist, um einen legitimen, gemeinwohlorientierten oder klar definierten Zweck (z. B. Forschung, Verbesserung von Systemen für medizinische Diagnose) zu erfüllen.
AI-Act	**Anbieter-Betreiber-Umkehr:** Nach der DS-GVO ist der Betreiber des KI-Systems für die Einhaltung der Datenschutzbestimmungen verantwortlich. Der AI Act legt die Hauptpflichten beim Anbieter des KI-Systems. Dies kann zu Unsicherheiten bei der Haftung führen, z. B. bei Fehlern in Hochrisiko-KI-Systemen. In einigen Fällen können Anbieter und Betreiber gemeinsam haftbar sein. Hier fehlt eine klare Koordinierung der Verantwortlichkeiten.	Klarstellungen sowohl in KI-VO als auch DS-GVO denkbar.
AI-Act	**Dopplung bei Meldepflichten an die Aufsichtsbehörden:** Art. 33 DS-GVO: Meldung von Datenschutzverletzungen an die Aufsichtsbehörde – Meldung innerhalb von 72 Stunden, Bei hohem Risiko auch an die betroffene Person (Art. 34 DS-GVO) Art. 73 AI Act: Anbieter von Hochrisiko-KI-Systemen sind verpflichtet, ein System zur kontinuierlichen Überwachung ihrer Systeme einzurichten und schwerwiegende Vorfälle, die die Sicherheit oder Gesundheit beeinträchtigen können, zu melden. Wenn ein Vorfall in einem KI-System gleichzeitig zu einer Datenschutzverletzung führt (z. B. unbefugter Zugriff oder Verlust personenbezogener Daten), greifen sowohl die Meldepflichten aus Artikel 33, 34 DS-GVO als auch die Vorfallmeldungen aus 61 AI Act → Möglicherweise Doppelmeldungen	Regelung zur Vermeidung von Doppelmeldepflichten.

Rechtsakt	Problem	Mögliche Lösung
AI-Act	**Überschneidung IT-Sicherheits-Anforderungen:** Art. 32 der DS-GVO und Art. 16 des AI Act gehen Hand in Hand, da beide von den Verantwortlichen verlangen, geeignete Sicherheitsmaßnahmen zu treffen, ohne dass das Verhältnis der Vorschriften zueinander geklärt ist.	Hier sollten Berichtspflichten zusammengelegt werden.
AI-Act	**Divergierende Hochrisiko-Klassifizierung:** Hochrisiko-Anwendungen nach dem AI Act und solche mit hohem Risiko nach der DS-GVO sind nicht deckungsgleich. KI-gestützte Profiling-Systeme gelten fast immer als Hochrisiko unter der DS-GVO, aber nicht zwangsläufig unter dem AI Act (vgl. Art. 5 Abs. 1 d) AI Act).	Integration der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO mit den Grundrechte-Risikoanalysen nach Art. 27 des AI Act.
DSA und DMA	**Divergierende Profiling Regelungen:** Es besteht eine Vielzahl von Vorschriften zu Profiling, die nicht abschließend aufeinander abgestimmt sind (vgl. EwG 71, Art. 22 DS-GVO, EwG 72, Art. 15 Abs. 1 des DMA und EwG 68 ff., Art. 26 Abs. 3, Art. 28 Abs. 2, Art. 38 des DSA)	
DSA und DMA	**Konflikte zwischen Transparenzpflichten und Datensparsamkeit:** Konflikte zwischen Transparenzpflichten (vgl. das, DMA und P2B-VO) und dem DS-GVO-Grundsatz der Datensparsamkeit und Datenminimierung nach Art. 5 Abs. 1 c) DS-GVO.	Offen
DS-GVO_DORA-VO	Pseudonymisierte Daten Art. 16 Abs. 5 RTS Risikomanagement zur DORA-VO	DORA-VO steht im fachlichen Widerspruch zur DS-GVO

Rechtsakt	Problem	Mögliche Lösung
	Pseudonymisierte Daten dürfen in Nichtproduktionsumgebungen gespeichert werden. Erwägungsgrund 26 DS-GVO Pseudonymisierte Daten gelten als personenbezogene Daten	Nach DORA darf etwas getan werden, das in der Regel datenschutzrechtlich unzulässig ist.
DORA-VO und Solvency II Dopplung	Anzeige Ausgliederung gemäß § 32 und 47 Nr. 8 VAG und, parallel Anzeigepflichten gemäß Artikel 28 Abs.3 DORA-VO Meldung von schweren IKT-Vorfällen an die BaFin gemäß Art. 19 DORA-VO, parallel Anzeigepflicht gemäß § 47 Nr. 9 VAG	Derselbe Sachverhalt wird nach zwei verschiedenen »Rechts-Regimes« an dieselbe Aufsichtsbehörde gemeldet.
AI-Act und Data Act	Eine einheitliche Dokumentation von Verarbeitungstätigkeiten und Produkt-/Daten-Inventarisierung schaffen.	
ePrivacy Richtlinie	**Unterschiedliche Meldeverpflichtungen bei Datenschutzvorfällen:** Datenschutzvorfälle müssen gem. Artikel 33 DS-GVO innerhalb von 72 Stunden an die zuständige Datenschutzaufsichtsbehörde gemeldet werden. Datenschutzvorfälle im Bereich der elektronischen Kommunikation müssen gem. §169 TKG i.V.m. VO 611/2023 EU hingegen innerhalb von 24 Stunden an die BNetzA und die BfDI gemeldet werden.	Beseitigung sektorspezifischer Sonderreglungen für die elektronische Kommunikation.

3 Zwischen AI Act und ...

Rechtsakt	Problem	Mögliche Lösung
Medizinprodukte-verordnung	**Ungenügende Abstimmung der Risikoklassifizierungen:** Nach der KI-Verordnung gelten alle KI-Systeme, die entweder selbst drittzertifizierungspflichtige Produkte sind oder Sicherheitskomponenten eines solchen Produkts gem. Anhang Ia AI Act darstellen, als Hochrisiko-KI-Systeme. Zu den Verordnungen und Richtlinien, die unter Anhang Ia fallen, zählt jedoch auch die Medizinprodukteverordnung. Diese legt fest, dass Softwareprodukte im medizinischen Bereich unabhängig von ihrem inhärenten medizinischen Risiko drittzertifizierungspflichtig sind. Folglich werden solche Softwareprodukte ausnahmslos in die Hochrisiko-Klasse des AI Acts eingeordnet, unabhängig von ihrem tatsächlichen Gefährdungspotenzial. Das Zusammenspiel der Regel 11 der MDR mit der Risikoklassifizierung nach der KI-Verordnung steht dem risikobasierten Ansatz beider Regelwerke entgegen und stellt für medizinisch unbedenkliche Produkte eine unverhältnismäßige regulatorische Belastung dar. Es bedarf einer Klärung dieses Umstands auf EU-Ebene.	Offen
Finanzen	Es fehlt eine Norm, die regelt, welche Elemente der Anforderungen an Daten und Daten Governance (Art. 10 AI Act) für Hochrisiko-KI-Systeme im Finanzbereich bereits durch die Daten-Governance-Anforderungen nach Artikel 174 der Capital Requirements Regulation (CRR) abgedeckt werden. Zudem ist unklar, inwieweit bestehende Dokumentations- und Transparenzanforderungen im Bankensektor, wie beispielsweise durch die MaRisk, die Vorgaben des AI Acts bereits erfüllen. Gleiches gilt für die Anforderungen an Cybersicherheit nach DORA.	Rechtssicherheit im Sinne von möglichst weitgehender Anrechenbarkeit von bestehenden Praktiken nach sektoraler Regulierung und Regelung zur Vermeidung von Doppelberichterstattungspflichten schaffen.
DSM-RL/ Urheberrecht der EU	Verweis auf einzelne Bestimmungen der DSM-RL grundsätzlich ok. Problem: mit Erwägungsgrund 106 liegt in einem Produktsicherheitsregulierungs-gesetz wie dem AI Act eine Vorschrift vor, die diametral gegen den	TBD: ErwG steht im Zusammenhang mit Art. 53 KI-VO. Nach Art. 53 KI-VO wird der Anbieter verpflichtet.

Rechtsakt	Problem	Mögliche Lösung
	urheberrechtlichen Grundsatz des Territorialitätsprinzips steht. Offen ist, ob es sich dabei um eine sicherheitsrechtliche oder eine urheberrechtliche Bestimmung handelt – das hat u.a. eine wesentliche Auswirkung darauf, wer die »Pflicht« aus EwG 106 einklagen kann.	
Maschinen-verordnung	**Unterschiedlicher Umgang mit dem Begriff des Sicherheitsbauteils:** Nach dem AI Act ist ein KI-System als Sicherheitsbauteil immer nur als Teil eines Produkts Gegenstand der Regulierung, während die Maschinenverordnung die Regulierung eines Sicherheitsbauteils stets separat vom Produkt vorsieht.	Offen
Produkthaftungs-RL	Verstößt ein Unternehmen gegen den AI Act, führt dies in der Regel auch zu einer Haftung nach Produkthaftungsrecht oder allgemeinem Deliktsrecht. Allerdings könnten Unternehmen in Einzelfällen auch trotz Erfüllung des AI Act haftbar sein. Dies würde für Unternehmen doppelte und potenziell widersprüchliche Anforderungen bedeuten.	Offen
Product Liability Guideline	Wann ist ein AI Modell ein Produkt, insb. wenn es sich nicht um ein AI System handelt. Genügt das Inverkehrbringen oder ist Inbetriebnahme erforderlich? Im R&D Bereich hoch relevant	Sobald es eine Zweckbestimmung zur Inbetriebnahme gibt im Sinne einer konkreten Anwendung.

4 Zwischen Data Act und …

Rechtsakt	Problem	Mögliche Lösung
DS-GVO	Mit der Abgrenzung von personenbezogenen und nicht-personenbezogenen Daten zwischen DA und DS-GVO gehen in hohem Maße unterschiedliche Folgen einher. Diese Abgrenzung ist häufig nicht sicher und führt in der Folge zu bedeutenden Compliance-Risiken. Der Data Act enthält keine Rechtsgrundlage für die Verarbeitung, was gilt damit bei Mischdatensätzen? (s.o.)	Im Data Act eine Rechtsgrundlage nach DS-GVO für die Verarbeitung personenbezogener Daten einführen. Nach Erwägungsgrund 34 gilt die DS-GVO. Eine Regelung im Verordnungstext und nicht nur im Erwägungsgrund wäre wünschenswert.
DS-GVO	Dritten ist nach Art. 6 (2) b) DA das Profiling auf Basis der erhaltenen Daten regelmäßig untersagt. Diese Regelung gilt unbeschadet von Art. 22 (2) a) + c) und EwG 71 DS-GVO. Je nach Auslegung von Art. 6 (2) b) DA, Art. 22 (2) a) und c) DS-GVO könnten die Regeln für Profiling bei nicht-personenbezogenen Daten strenger sein als bei personenbezogenen Daten, was nicht nahliegend ist.	Art. 6 (2) b) DA kritisch evaluieren und ggf. löschen bzw. zumindest an DS-GVO angleichen.
AI Act	Art. 10 AI Act regelt Anforderungen an Datenqualität, Data Management, Data-Governance in Bezug auf High-Risk AI-Systeme. Es ist unklar, wie sich diese Anforderungen zu den Data-Governance-Anforderungen in Art. 33 Data Act verhalten und wie die beiden Regelungsbereiche jeweils operationalisiert werden.	Offen
Art. 101 f. AEUV (Kartellverbot)	Es ist nicht abschließend klar, wie sich die Datenteilungsansprüche gem. Kapitel II DA und hier insb. den Ausnahmen in Art. 4 (6) ff. sowie Art. 5 (9) ff. DA zum Kartellverbot gem. Artikel 101 und 102 AEUV (engl. TFEU) und insb. auch HBER Guidelines Kapitel VI (Information Exchange) verhalten. Ersterer Bereich fordert die Offenlegung auch sensibler Daten inkl. Geschäftsgeheimnissen unter bestimmten Umständen, letzterer Bereich hat insb. das Ziel, den Austausch sensibler Daten zu verbieten. EwG 116 DA beantwortet diese Frage auf den ersten Blick (»Diese Verordnung sollte die Anwendung der Wettbewerbsvorschriften, insbesondere der Artikel 101 und 102 AEUV unberührt lassen. Die in dieser Verordnung vorgesehenen	Klarstellen, dass im Konfliktfall die kartellrechtlichen Vorschriften nach dem AEUV vorrangig anzuwenden ist.

Rechtsakt	Problem	Mögliche Lösung
	Vorschriften dürfen nicht dazu verwendet werden, den Wettbewerb entgegen den Vorschriften des AEUV einzuschränken.«). Auf den zweiten Blick ist streitig, ob EwG 116 DA jegliche Weitergabe insb. von Geschäftsgeheimnissen an Dritte verbietet, da dann die sog. Handbrake-Mechanisms (Art. 4 6) ff., Art. 5 9) ff. DA) in den intendierten Fällen (u.a. Zugriff auf sensible Daten durch Wettbewerber unbedingt vermeiden) unnötig wären.	
Data Act	Bei den vorvertraglichen Informationspflichten aus Art. 3 Abs. 2, 3 DA sind Sprache und Umfang unklar. Ungeklärt ist zudem die Vereinbarkeit mit anderen Informationspflichten.	Spätestens auf behördlicher Ebene klarstellen, dass vorvertragliche Informationspflichten mit Informationspflichten aus anderen EU-Rechtsaktenkombiniert werden dürfen und diese lediglich in Englisch vorliegen müssen.
Data Act	Bei dem Vertragserfordernis gem. Artikel 4 Abs. 13 DA sind Sprache und Umfang unklar. Zudem bleibt die Frage offen, ob die Datenübermittlungsverträge mit anderen Klauseln kombiniert werden können. Aus Art. 5 DA wird zudem nicht ersichtlich, dass auch zwischen Dateninhabern und Datenempfängern ein Vertragsverhältnis erforderlich ist.	Spätestens auf behördlicher Ebene klarstellen, dass Vertrag mit anderen Verträgen kombiniert werden darf und dieser lediglich in Englisch vorliegen muss. Hinweis: Die EU Kommission hat bereits versucht durch Musterverträge nach Art. 41 DA Abhilfe zu schaffen.
Data Act	Art. 9 Abs. 7 DA: Informationspflichten ggü. Datenempfängern. Integration mit anderen Informationspflichten? Sprache? Umfang?	Spätestens auf behördlicher Ebene klarstellen, dass Informationspflichten mit anderen Informationspflichten kombiniert werden dürfen und diese lediglich in Englisch vorliegen müssen.
Data Act	Art. 26 DA: Informationspflicht zu Wechselmethoden und Online-Register. Integration mit anderen Informationspflichten? Sprache? Umfang?	Spätestens auf behördlicher Ebene klarstellen, dass Informationspflichten mit anderen Informationspflichten kombiniert werden dürfen und diese lediglich in Englisch vorliegen müssen.
Data Act	Artikel 28: Transparenzpflichten für Anbieter auf deren Website. Integration mit anderen Informationspflichten? Sprache? Umfang?	Spätestens auf behördlicher Ebene klarstellen, dass Informationspflichten mit anderen Informationspflichten kombiniert werden dürfen und diese lediglich in Englisch vorliegen müssen.

5 Zwischen NIS-2-RL und ...

Rechtsakt	Problem	Mögliche Lösung
Data Act	Der Data Act verpflichtet zur Offenlegung von Daten, auch in sicherheitskritischen Kontexten. Dies kann den Anforderungen der NIS-2-RL zur Vertraulichkeit und Verschlüsselung entgegenstehen. Besonders bei kritischen Infrastrukturen können Datenzugriffe Risiken für Cybersicherheit schaffen, wenn keine einheitliche Regulierung vorhanden ist.	Klarstellen, dass im Konfliktfall nationale Umsetzung der NIS-2-RL vorrangig anzuwenden ist.
CRA	NIS2-RL erlaubt die Einführung delegierter Rechtsakte gem. Art. 24 (2) NIS-2-RL über die obligatorische Verwendung von zertifizierten IKT-Produkten. Dies kann sich direkt mit den CRA überschneiden und den Verwaltungsaufwand erhöhen.	CE-Kennzeichnung unter Anwendung des CRA sollte als Anforderung für die IKT-Produkte ausreichend sein.
DS-GVO	Erhebliche Sicherheitsvorfälle gem. NIS-2-RL können gleichzeitig einen Datenschutzvorfall nach DS-GVO darstellen. Somit müssen betroffene Unternehmen in Deutschland an verschiedene Stellen gebunden. NIS2 fokussiert sich auf die Wiederherstellung der Informationssicherheit und Cybersicherheit, während die DS-GVO den Schutz der Rechte und Freiheiten natürlicher Personen sowie deren Befähigung zur Risikominimierung in den Mittelpunkt stellt. Dies kann zu Konflikten führen, wenn beide Vorschriften für denselben Vorfall einzuhalten sind.	DS-GVO und NIS2 haben unterschiedliche Schutzgüter. Besser als ein pauschaler Vorrang von NIS2 wäre eine einheitliche Meldung.

6 Zwischen CRA und …

Rechtsakt	Problem	Mögliche Lösung
u.a. DS-GVO/ NIS-2-RL	**Berichtspflichten (DS-GVO, NIS-2-RL etc.):** Art. 14 (1) und (3) CRA verpflichtet Hersteller schwerwiegende Vorfälle, die sich auf die Sicherheit des Produkts auswirken, und aktiv ausgenutzte Schwachstelle an ENISA zu melden. Dies verursacht eine mögliche Überlappung mit Art. 33 DS-GVO und Art. 7, 21 NIS-2-RL.	Klarstellen, welche Rechtsgrundlage im Konfliktfall vorrangig anzuwenden ist. Idealerweise einen 1-Stop-Shop zur Meldung einführen.
DORA	Unternehmen im Finanzsektor, insbesondere solche, die digitale Dienstleistungen oder Produkte anbieten, können unter mehrere Vorschriften gleichzeitig fallen, was zu sich überschneidenden Compliance-Anforderungen führt.	Mit Hilfe von delegierten Rechtsakten feststellen, dass DORA im Überschneidungsfall als lex specialis vorrangig ist.
AI Act	Überlappung und mögliche Inkonsistenzen bei Cybersicherheitsanforderungen zwischen AI Act und CRA Mögliche Überschneidungen und Widersprüche zwischen Art. 15 CRA zu Genauigkeit, Robustheit und Cybersicherheit für KI-Systeme und den Anforderungen des CRA.	Harmonisierung der Standardisierungsarbeiten
ÖkodesignVO	Updates von Software und Firmware dürfen nicht zu einer Leistungsverschlechterung des Produkts führen. Daraus ergibt sich ein Zielkonflikt mit dem Cyber Resilience Act.	
NIS2	Einheitliches Verständnis von direktem oder indirektem materiellem Schaden.	

7 Zwischen DMA und ...

Rechtsakt	Problem	Mögliche Lösung
DS-GVO	**Zielkonflikt von Diensteöffnung zu Sicherheits-/Schutzvorschriften:** Verschiedene Zugangsansprüche und Interoperabilitätspflichten im DMA können im Konflikt zu Cybersecurity- und DS-GVO-Vorschriften (bspw. Privacy by Design) stehen, wenn die (neueren) DMA-Vorschriften nicht vor dem Hintergrund der bestehenden Regularien ausgelegt werden.	Offen
Data Act, DSA und P2B-VO	Dark Patterns (s.o.), Profiling (s.o.) und eine Vielzahl sonstiger Überschneidungen	s.o.

8 Zwischen DSA und …

Rechtsakt	Problem	Mögliche Lösung
DS-GVO	Im DSA existiert eine Reglung bzgl. eines Verbots des Einsatzes von Dark Patterns, die wiederum auf die Ausgestaltung von Cookie-Bannern Anwendung findet. Hier ist jedoch das Verhältnis zur DS-GVO nicht klar/ eindeutig. Die EU behilft sich diesbezüglich stets mit dem Hinweis, dass Vorgaben aus der DS-GVO/aus anderen Rechtsakten keine Anwendung finden. Diese widersprechen z. T. den neuen Vorgaben. Die unberührt-Regelung in Art. 2 Abs. 4 g) DSA hilft insoweit nicht weiter.	Offen
P2B-VO	Zunächst ergeben sich aus den Begriffen in Art. 2 Nr. 2 P2B-VO und Art. 3 a) DSA Abweichungen. Zudem gibt es Überschneidungen zwischen Art- 20, 21 DSA und Art. 11 und 12 P2B-VO. Die unberührt-Regelung in Art. 2 Abs. 4 e) DSA hilft insoweit nicht weiter.	Offen
UGP-RL	Nach Art. 25 Abs. 2 DSA gilt das Verbot von sog. »Dark Patterns« nicht für Praktiken, die unter die UGP-RL 2005/29/EG fallen. Jedoch bleibt unklar, worin in diesem Fall der Restanwendungsbereich der Regelung bestehen soll.	Offen

9 Zwischen DGA und …

Rechtsakt	Problem	Mögliche Lösung
Data Act	Ein Unternehmen kann gleichzeitig sowohl a) Anbieter eines Datenvermittlungsdienstes gem. Art. 2 Nr. 11, Art. 10 ff. DGA, b) datenaltruistische Organisation gem. Art. 2 Nr. 16, Art. 16 ff. DGA als auch c) Betreiber eines Datenraums gem. DA Art. 33 sein. Ebenfalls wäre denkbar, dass der Datenraum oder bspw. ein System darin als Datenverarbeitungsdienst gem. Art. 2 Nr. 8 DA gilt. Während mit a), b) und c) unmittelbar unterschiedliche Rechte und Pflichten einhergehen, liegen die Rechte und Pflichten bei d) bei den Teilnehmern eines solchen Datenraums, was wiederum mit hoher Wahrscheinlichkeit auch bestimmte Anpassungen seitens des Betreibers des Datenraums erfordern wird. In Summe sind also alleine gemäß Data Act und DGA unter Umständen 4 Konzepte gleichzeitig auf ein Unternehmen anwendbar, ohne dass deren Verhältnis zueinander erklärt oder strukturiert würde.	Das Konzept von Datenvermittlungsdiensten im DGA durch das Konzept von Data Spaces ersetzen. Das Konzept von datenaltruistischen Organisationen beibehalten. Klarstellen, dass Entitäten Data Space sein können oder alternativ, ersatzweise datenaltruistische Organisationen oder weder noch. Die Ziele und unterliegenden Prinzipien des DGA müssen erhalten bleiben.
Data Act	Art. 12 (d) DGA regelt, dass der Anbieter eines Datenintermediationsdienstes den Datenaustausch unterstützen und Daten unter Umständen in bestimmte Formate konvertieren soll. Art. 33 (1) DA wiederum regelt insb., dass die Beschreibung von »Datenstrukturen, Datenformate[n], Vokabulare[n], Klassifizierungssysteme[n] [etc.]« durch den Teilnehmer an Datenräumen erfolgen soll. Vor diesem Hintergrund ist unklar, wieso beides parallel gefordert wird.	Auflösung über Angleichung des materiellen Anwendungsbereichs: Datenvermittlungsdienste im DGA durch Konzept von Data Spaces ersetzen.
Data Act	Art. 12 (j) DGA regelt, dass der Anbieter eines Datenvermittlungsdienstes bestimmte Maßnahmen ergreifen muss, um rechtswidrigen Transfer von nicht-personenbezogenen Daten in Drittstaaten zu vermeiden. Insofern ein Datenvermittlungsdienst oder Subsysteme davon (bspw. für Pseudonymisierung oder temporäre Speicherung, vgl. Art. 12 (e) DGA) als Datenverarbeitungsdienst gem. DA gelten, sind auch die Pflichten zur Vermeidung rechtswidriger Transfers von oder Zugriff auf nicht-personenbezogene Daten gem. Art. 32 DA anwendbar. Deren Verhältnis zueinander ist weder erklärt noch strukturiert.	Bzgl. technischer organisatorischer Maßnahmen von Art. 12 j DGA auf jene aus Art. 32 DA verweisen.

Rechtsakt	Problem	Mögliche Lösung
DS-GVO	Es ist unklar, wie sich Art. 12 (j) DGA und die DS-GVO zueinander verhalten. Ersteres schützt nicht-personenbezogene Daten, letzteres schützt personenbezogene Daten. Dies ist ein Problem, wenn sowohl personen- als auch nicht-personenbezogenen Daten parallel verarbeitet werden und eine Trennung faktisch nicht möglich ist. Mit der Abgrenzung von personenbezogenen und nicht-personenbezogenen Daten zwischen DGA und DS-GVO gehen in hohem Maße unterschiedliche Folgen einher. Diese Abgrenzung ist häufig nicht sicher und führt in der Folge zu bedeutenden Compliance-Risiken.	Klare, rechtsverbindliche Vorgaben zu Pseudonymisierung und Anonymisierung verfügbar machen.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Ansprechpartnerin

Isabelle Stroot | Referentin Datenschutz

T +49 30 27576-228 | i.stroot@bitkom.org

Verantwortliches Bitkom-Gremium

AK Datenschutz

Copyright

Bitkom 2025

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.

bitkom.org