Für einen funktionierenden digitalen Binnenmarkt

Regulatorische Inkohärenzen und Doppelregulierungen abbauen

Die Von-der-Leyen-Kommission hat die vertiefte Integration des europäischen digitalen Binnenmarkts ins Zentrum ihres Handelns gerückt und entsprechend die 2020er Jahre zur Digitalen Dekade Europas ausgerufen. In diesem Kontext hat die europäische Kommission eine Vielzahl an regulatorischen Maßnahmen ergriffen, um die Entwicklung von digitalen Technologien und den Aufbau eines Datenökosystem unter Wahrung europäischer Werte und Rechte zu fördern. Viele der in diesem Rahmen geplanten Gesetzesakte sind mittlerweile verabschiedet, die Umsetzungsfristen für Unternehmen laufen bereits (siehe Abb.1).

Die digitale Integration des europäischen Binnenmarktes birgt ein enormes wirtschaftliches und gesellschaftliches Wertschöpfungspotenzial und hilft bei der Realisierung der europäischen Nachhaltigkeitsziele. Europa kann dabei als globaler Akteur im digitalen Zeitalter gestärkt werden. Für die Elektro- und Digitalindustrie, deren Unternehmen bis 2026 voraussichtlich zwei Drittel ihres Umsatzes mit digital veredelten Produkten und digitalen Dienstleistungen erwirtschaften werden, ist die vertiefte Integration des europäischen Digital-Binnenmarkts Voraussetzung für ihre zukünftige Wettbewerbsfähigkeit.

Aus Sicht der Industrie sind die zentralen regulatorischen Elemente zur Erreichung der Kommissions-Ziele umfänglich erfasst. **Es bedarf daher momentan keiner zusätzlichen Regulierung – weder auf europäischer Ebene noch auf nationaler Ebene**. Die Kommission und auch die Bundesregierung sollten den Unternehmen in der kommenden Legislaturperiode ausreichend Zeit geben und dabei unterstützen, die neuen Regulierungen zu implementieren und in deren Rahmen neue Geschäftsmodelle zu entwickeln. Die zunehmende Regulierungsdichte, regulatorische Inkohärenzen, Doppelregulierungen und Dysfunktionalitäten in der Europäischen Digitalpolitik sind besondere Herausforderungen für die Unternehmen der Elektro- und Digitalindustrie. Dies führt nicht nur zu Rechtsunsicherheiten und damit verbundenen administrativen Kosten, sondern auch zur unnötigen Benachteiligung gegenüber Drittländern, oder schlichter Nichtumsetzbarkeit und Desinvestitionen.

Die Aufgabe der kommenden EU-Kommission sowie der Bundesregierung sollte es daher sein, **bestehende Regulierungen so weiterzuentwickeln, dass regulatorische Inkohärenzen und Doppelregulierungen beseitigt und Innovationen angereizt werden.** Auch sollte im Sinne der Rechtssicherheit für alle Wirtschaftsakteure darauf hingewirkt werden, dass zukünftige gesetzliche Anforderungen von Vorneherein klar und widerspruchsfrei gestaltet werden. Nur so wird vermieden, dass Klarstellungen in rechtlich nicht verbindlichen Leitfäden aufgelöst werden müssen. Bei bestehenden Doppelregulierungen zum selben Tatbestand ist zwingend zu klären, welcher Rechtsakt Vorrang hat. Eine klare Abgrenzung der jeweiligen Geltungsbereiche und der grundlegenden Anforderungen, sowie klare Vorgaben, nach welchem Rechtsakt das Konformitätsbewertungsverfahren durchzuführen ist, sind essenziell.

Viele der genannten Rechtsakte verweisen für das Inverkehrbringen von Produkten auf den New Legislative Framework (NLF) ((EU) 768/2008). Dieser bietet einen konsistenten Rechtsrahmen mit gemeinsamen Definitionen, Mustervorgaben und Mindestanforderungen. Insbesondere in Fällen, in denen vom NLF abgewichen wird, bzw. im Zusammenspiel mit Rechtsakten, die nicht in die Systematik des NLF fallen, ergeben sich jedoch regelmäßig Abweichungen, die zu Unsicherheiten und erhöhtem bürokratischen Aufwand bei der Inverkehrbringung im europäischen Binnenmarkt führen. Der NLF sollte daher gestärkt werden, indem seine Systematik grundlegend bei dem Inverkehrbringen von Produkten Anwendung findet.

Ziel des vorliegenden Dokuments ist es, Regulierern auf nationaler und europäischer Ebene Hilfestellung zu geben, um faktenbasierte Entscheidungen bei der Priorisierung möglicher Reformvorhaben in der Digitalpolitik zu treffen. Die schwerwiegendsten regulatorischen Fälle aus Sicht der Elektro- und Digitalindustrie haben wir daher in den Kategorien „worst cases“ und „heavy cases“ zusammengestellt. Hier sehen wir den dringlichsten Handlungsbedarf, da ohne eine Weiterentwicklung bzw. Anpassung der Rechtsakte, Unternehmen vor Rechtsuntersicherheiten und bürokratischen Aufwänden stehen oder im schlimmsten Fall ihre Produkte nicht mehr vermarkten können.

Dabei haben wir uns auf folgende Rechtsakte konzentriert:

- Datengesetz (Data Act)
- Datenschutzgrundverordnung (DSGVO)
- Funkanlagenrichtlinie (Radio Equipment Directive – RED)
- Gesetz über Cyberresilienz (Cyber Resilience Act – CRA)
- KI-Verordnung (AI Act)
- Maschinen-Verordnung (MVO)
- EU Ökodesign-Verordnung (Ecodesign for Sustainable Product Regulation – ESPR)
- 2. Richtline zur Netzwerk- und Informationssicherheit (NIS-2-RL)

Die folgende Übersicht zeigt einen Zeitstrahl der wesentlichen EU-Rechtsakte und ihre jeweiligen Übergangszeiten. Es wird deutlich, vor welche zusätzlichen Herausforderungen europäische Unternehmen durch die massive Regulierungsdichte und teils sehr kurzen Übergangsfristen gestellt werden. Zumal die Anpassung von Produkten und Prozessen in der Regel auf harmonisierten Normen basiert, deren Vorliegen oftmals essenziell für das Inverkehrbringen der Produkte ist.[1]

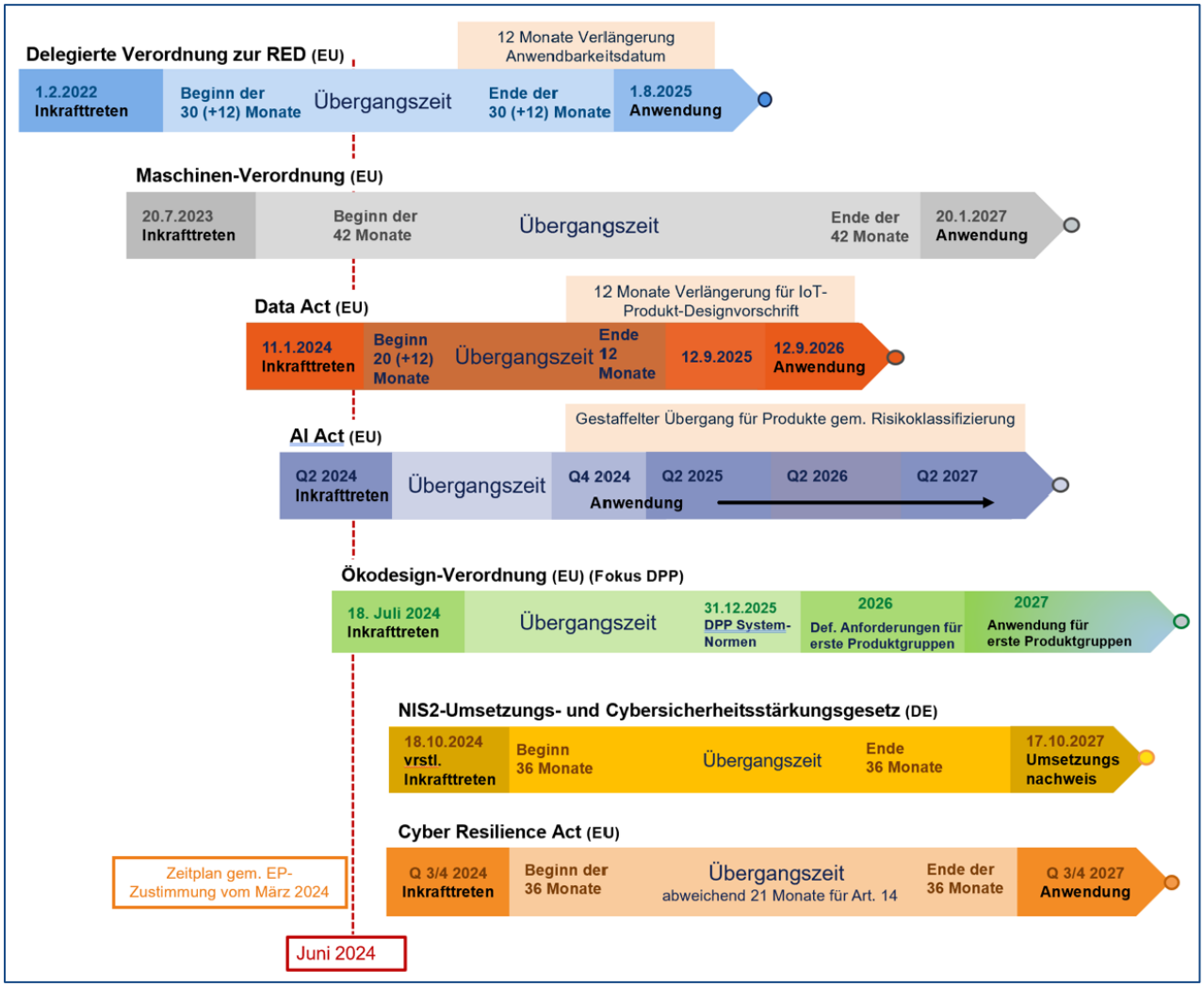

Abbildung 1: Zeitstrahl zu Übergangszeiten und zum Inkrafttreten wesentlicher EU-Rechtsakte in der Digitalwirtschaft (eigene Darstellung)

Abschließende Bemerkungen

Zum Redaktionsschluss waren noch nicht alle untersuchten Rechtsakte im Amtsblatt der europäischen Union veröffentlicht. Dementsprechend lagen auch noch nicht durchgängig alle Rechtstexte in der deutschen Übersetzung vor. Auch können sich in der Zwischenzeit Änderungen insbesondere in der Artikel-Nummerierung der nicht finalen Texte ergeben haben.

[1] ZVEI (2023): Funktionsfähiger EU-Binnenmarkt – angemessene Übergangsfristen sicherstellen

Worst cases
Regulatorische Widersprüche und Inkohärenzen

Im Falle eines regulatorischen Widerspruches können sich Unternehmen nicht an die Vorgaben eines Gesetzes halten, ohne gegen die Vorgaben eines anderen Gesetzes zu verstoßen. Im schlimmsten Fall ist ihr Handeln bzw. Nicht-Handeln sogar bußgeldbewehrt. Dies kann dazu führen, dass Unternehmen aufgrund der rechtlichen Unsicherheit innovative digitale Produkte nicht angehen.

Data Act vs. DSGVO

<table>
<tr><td>Zielkonflikt</td><td colspan="2">“Access by design” vs. “Privacy by design”

Die Vorgaben des Data Act, große Datenmengen – auch personenbezogene – möglichst umfangreich und einfach zugänglich zu machen, widerspricht dem präventiven Verbot der Weitergabe personenbezogener Daten der DSGVO, flankiert durch die datenschutzrechtlichen Grundsätze der Zweckbindung und Datenminimierung, sowie die datenschutzrechtlichen Löschpflichten im Datenschutzrecht.

Ganz offensichtlich zeigt sich dieser Konflikt am Beispiel der Designvorgaben. Während die DSGVO für (vernetzte) Produkte den Grundsatz “privacy by design / default” aufstellt, fordert der Data Act für die gleichen Produkte ein “access by design”.
Um eine rechtssichere Anwendung beider Verordnungen sicherzustellen, müssen diese Konflikte aufgelöst werden.</td></tr>
<tr><td>Bewertung und Empfehlung aus Sicht des ZVEI</td><td colspan="2">Der Schutz personenbezogener Daten, sowie das Recht des Einzelnen auf informationelle Selbstbestimmung sind hoch anzusiedeln und müssen garantiert bleiben. Gleichwohl ist der Austausch und die Nutzung von Daten für die deutsche und europäische Wirtschaft – insbesondere die datengetriebene Elektro- und Digitalindustrie – essenziell, um neue Technologien und Innovationen in den Markt zu bringen, und damit für eine nachhaltige Wertschöpfung zu sorgen. Vor diesem Hintergrund plädieren wir für einen „ermöglichenden“ Datenschutz und regen an, das grundsätzliche Verbotsprinzip der DSGVO zu überwinden. Zumindest jedoch müssen dringend die Erlaubnistatbestände so angepasst und ausgeweitet werden, dass die Verarbeitung von personenbezogenen Daten nicht mehr im Widerspruch zu den Zielen einer datengetriebenen Wirtschaft und den Vorgaben an das Produktdesign aus dem Data Act stehen.

Eine Verletzung der DSGVO wäre etwa die Nutzung personenbezogener Daten, welche über die Kenntnis und Genehmigung der betroffenen Person hinausgeht und weiteren kommerziellen Zwecken dient. Demgegenüber kann aber die Nutzung personenbezogener, nutzergenerierter Daten für die KI-Weiterentwicklung, oder die Verwendung als Trainingsdaten für KI-Modelle erforderlich sein. Diese entwicklungstechnische Nutzung darf keine weiteren Folgen oder Risiken für das Datensubjekt mit sich bringen, sollte aber für den genannten Zweck erlaubt sein.

Voraussetzung für einen ermöglichenden Datenschutz ist die Klarstellung zur Anonymisierung und Pseudonymisierung personenbezogener Daten im Artikeltext der DSGVO. „Ermöglichender“ Datenschutz würde beispielsweise bedeuten, dass klargestellt wird, dass der Anonymisierung ein relatives Verständnis zugrunde liegt, also dass eine Anonymisierung auch dann vorliegt, wenn eine Re-Identifizierbarkeit der betroffenen Person nicht gänzlich ausgeschlossen ist, aber aufgrund eines unverhältnismäßig hohen Aufwands ausscheidet.</td></tr>
<tr><td>Betreffende Rechtsnormen</td><td><u>Data Act</u>

Erwägungsgrund 35
Im Gegensatz zu Artikel 20 der Verordnung (EU) 2016/679 wird mit der</td><td><u>DSGVO</u>

Art. 5
(1) Personenbezogene Daten müssen:</td></tr>
</table>

	vorliegenden Verordnung die technische Machbarkeit des Zugangs Dritter zu allen Arten von Daten, die in ihren Anwendungsbereich fallen – ob personenbezogen oder nicht-personenbezogen –, vorgeschrieben und gewährleistet, womit sichergestellt wird, dass technische Hindernisse den Zugang zu diesen Daten nicht mehr behindern oder verhindern. **Art. 3** (1) Vernetzte Produkte werden so konzipiert und hergestellt und verbundene Dienste werden so konzipiert und erbracht, dass die Produktdaten und verbundenen Dienstdaten – einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen relevanten Metadaten – standardmäßig für den Nutzer einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt zugänglich sind.	c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“); **Art. 25** (1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere, der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen, trifft der Verantwortliche, sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung, als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung –, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen, und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. (2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

CRA vs. ESPR

Zielkonflikt	**Schließen von Sicherheitslücken vs. Verhinderung von Leistungsverschlechterung** Im Cyber Resilience Act (CRA) gibt es die Vorgabe, dass Sicherheitslücken über Sicherheitsupdates geschlossen werden müssen. Die Ökodesign-Verordnung (ESPR) gibt vor, dass die Leistung eines Produkts durch Soft- oder Firmware-Updates nicht verschlechtert werden darf. Selbiges gilt auch in bereits existierenden Exekutivrechtsakten (“implementing measures“) der bisherigen Ökodesign-Richtlinie. Es besteht die Gefahr, dass notwendige mildernde Maßnahmen (“mitigating measures”), um ein Produkt CRA-konform zu halten, dazu führen könnten, dass diese als Verschlechterung der Leistung (“worsening performance”) eines Produkts angesehen werden und damit das Produkt nicht mehr konform mit der ESPR wäre.

Bewertung und Empfehlung aus Sicht des ZVEI	Wenn Produkte sowohl unter die ESPR als auch unter die Risikoklassifizierung des CRA fallen, dann ist bei der Formulierung der Delegated Acts der ESPR darauf zu achten, dass Produktfunktionalitäten und ggf. die Leistung eines Produkts zur Schließung von Sicherheitslücken (zur Erfüllung der Vorgaben aus dem CRA) eingeschränkt werden dürfen.	
Betreffende Rechtsnormen	**CRA** **Art. 3** (30) 'substantial modification' means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Annex I, Part I, or which results in a modification to the intended purpose for which the product with digital elements has been assessed; **Annex I Essential Requirements Part I** (2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: […] (c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them; **Annex I Essential Requirements Part II** Manufacturers of products with digital elements shall: (2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;	**ESPR** **Art. 40** (5) Bei Messung mit der für die Konformitätsbewertung verwendeten Prüfmethode dürfen Software- oder Firmware-Aktualisierungen nicht dazu führen, dass sich die Produktleistung über das in den gemäß Artikel 4 erlassenen anwendbaren delegierten Rechtsakten angegebene akzeptable Maß hinaus in Bezug auf einen oder mehrere der in diesen delegierten Rechtsakten geregelten Produktparameter oder aus Sicht des Nutzers die Funktionsfähigkeit verschlechtert, es sei denn, der Kunde hat vor der Aktualisierung seine ausdrückliche Zustimmung zu einer solchen Leistungsverschlechterung erteilt. Die Ablehnung der Aktualisierung darf nicht zu einer Änderung führen. Software- oder Firmware-Aktualisierungen dürfen unter keinen Umständen zu einer Verschlechterung die in Unterabsatz 1 dieses Absatzes genannte Leistung in einem Maß führen, dass das Produkt den Anforderungen der gemäß Artikel 4 erlassenen delegierten Rechtsakte nicht mehr entspricht, die zum Zeitpunkt des Inverkehrbringens oder der Inbetriebnahme des Produkts galten. **Art. 2** (8) „Leistungsanforderung" eine quantitative oder nicht quantitative Anforderung an oder in Bezug auf ein Produkt zur Erreichung eines bestimmten Leistungsniveaus im Hinblick auf einen in Anhang I genannten Produktparameter; **Annex I Product parameters** Die folgenden Parameter können gegebenenfalls als Grundlage für die Verbesserung der in Artikel 5 Absatz 1 genannten Produktaspekte herangezogen und bei Bedarf ergänzt werden: (g) Verbrauch von Energie, Wasser und anderen Ressourcen in einem oder mehreren Abschnitten des Lebenszyklus des Produkts, einschließlich der Auswirkungen physischer Faktoren oder von Software- und Firmware-Aktualisierungen auf die

		Produkteffizienz sowie der Auswirkungen auf die Entwaldung;

Heavy cases
Dysfunktionales Zusammenspiel von Regulierungen, Doppelregulierung und rechtliche Unklarheiten

Sind verschiedene Regulierungen nicht aufeinander abgestimmt, können Regulierungsspitzen entstehen. Diese treffen überproportional einzelne Unternehmen oder Produktgruppen. Bei Unternehmen in den betroffenen Segmenten kommt es in der Folge zu Handlungshemmnissen und verminderter Innovationsaktivitäten sowie Verlagerungseffekten. Ähnliche Folgen können auftreten, wenn verschiedene Regulierungen denselben Tatbestand in unterschiedlicher Weise regeln oder unterschiedliche Definitionen zugrunde gelegt werden. Unternehmen stehen vor der Herausforderung, dass Produkte ggf. nach unterschiedlichen Vorgaben gestaltet werden müssen. Teilweise schreiben Rechtsakte auch unterschiedliche Meldewege für denselben Sicherheitsvorfall vor. All dies führt mindestens zu einem erhöhten bürokratischen Aufwand, höheren Produktionskosten und einer Verlangsamung des Innovationsprozesses.

Data Act vs. NIS-2-Richtlinie

Zielkonflikt	**Verpflichtung zur Datenoffenlegung vs. Security-Anforderungen von Einrichtungen** Grundsätzlich sind gemäß Data Act dem Nutzer oder Dritten die durch die Nutzung entstandenen Daten bereitzustellen. Nutzer und Dateninhaber können den Zugang sowie die Nutzung oder die erneute Weitergabe von Daten vertraglich beschränken oder untersagen, wenn die Weitergabe schwerwiegende nachteilige Auswirkungen auf die Gesundheit oder die Sicherheit von natürlichen Personen haben könnte. Nicht explizit eingeschränkt wird hingegen die Verpflichtung zur Datenoffenlegung, insofern sie die Sicherheit von Objekten, Einrichtungen oder Organisationen betrifft. Dabei können Daten von bösartigen Akteuren („malicous actors“) für (Cyber)-Angriffe genutzt werden, besonders wenn die geteilten Daten Rückschlüsse auf Prozesse, Systeme und Architekturen von Organisationen erlauben. Die Security einer Einrichtung sollte daher Vorrang vor Verpflichtungen zum Datenteilen haben. Dies gilt insbesondere für Einrichtungen im Bereich der kritischen Infrastrukturen. Zudem stellt die NIS-2-Richtlinie Anforderungen an Risikomanagement-Maßnahmen hinsichtlich Vertraulichkeit, besonders Verschlüsselung und Authentifizierung, die den Anforderungen des einfachen und hürdenlosen Zugangs zu Daten aus dem Data Act entgegenstehen könnten. Zwar findet der Data Act in den Zuständigkeiten der Mitgliedstaaten in Bezug auf die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit ihre Schranken. Es bleibt jedoch den Mitgliedstaaten vorbehalten, ob und inwiefern nicht nur Betreiber, sondern auch bereits Zulieferer hierunter fallen. Eine unterschiedliche Auslegung in den EU-Mitgliedstaate kann Rechtsunsicherheiten und enorme Marktanpassungskosten insbesondere für KMU nach sich ziehen.
Bewertung und Empfehlung aus Sicht des ZVEI	Es bedarf einer Klarstellung im Data Act, dass die Verpflichtung zur Datenoffenlegung, insofern sie die Sicherheit von Objekten, Einrichtungen oder Organisationen betrifft, vergleichbar dem Schutz von natürlichen Personen, eingeschränkt werden kann. Bezüglich der Anwendung des Data Acts für kritische oder sensible Bereiche, Sektoren oder Infrastrukturen sollte die EU-Kommission zeitnah Empfehlungen zur harmonisierten Umsetzung in den Mitgliedsstaaten erlassen.

Betreffende Rechtsnormen	**<u>Data Act</u>** **Art. 3** (1) Vernetzte Produkte werden so konzipiert und hergestellt und verbundene Dienste werden so konzipiert und erbracht, dass die Produktdaten und verbundenen Dienstdaten – einschließlich der für die Auslegung und Nutzung dieser Daten erforderlichen relevanten Metadaten – standardmäßig für den Nutzer einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, direkt zugänglich sind. **Art. 4** (2) Nutzer und Dateninhaber können den Zugang zu sowie die Nutzung oder die erneute Weitergabe von Daten vertraglich beschränken, wenn eine solche Verarbeitung die im Unionsrecht oder im nationalen Recht festgelegten Sicherheitsanforderungen des vernetzten Produkts beeinträchtigen und damit zu schwerwiegenden nachteiligen Auswirkungen auf die Gesundheit oder die Sicherheit von natürlichen Personen führen könnte. Die für die betreffenden Sektoren zuständigen Behörden können den Nutzern und Dateninhabern in diesem Zusammenhang technisches Fachwissen bereitstellen. Verweigert der Dateninhaber die Weitergabe von Daten gemäß diesem Artikel, so teilt er dies der gemäß Artikel 37 benannten zuständigen Behörde mit **Erwägungsgrund 10** Die vorliegende Verordnung gilt nicht für nicht unter das Unionsrecht fallende Bereiche und berührt nicht die Zuständigkeiten der Mitgliedstaaten in Bezug auf die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, die Zoll- und Steuerverwaltung oder die Gesundheit und Sicherheit der	**<u>NIS-2</u>** **Art. 21** 1. Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten. Die in Unterabsatz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, dass dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen. 2. Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen: a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme; b) Bewältigung von Sicherheitsvorfällen; c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement; d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte

	Bürgerinnen und Bürger, unabhängig von der Art des Rechtsträgers, der von den Mitgliedstaaten mit der Wahrnehmung von Aufgaben im Zusammenhang mit diesen Zuständigkeiten betraut wurde.	der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern; e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen; f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit; g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit; h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung; i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen; j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

CRA vs. RED

Zielkonflikt	**Doppel-Regulierung in CRA und RED** Der technische Regelungsgehalt der delegierten Verordnung (EU) 2022/30 unter der Funkanlagenrichtlinie (Artikel 3.3 d,e,f) und des CRA (vgl. Annex I) haben eine große Schnittmenge, da sie denselben Aspekt – die Sicherheit vernetzter Produkte – regulieren. Es ist daher wichtig, dass sich die konkreten Anforderungen in harmonisierten Normen unter dem Cyber Resilience Act an denen orientieren, die in den (prEN) 18031-1,-2,-3 unter der delegierten Verordnung (EU) 2022/30 unter der RED an Produkte festgelegt werden.
Bewertung und Empfehlung aus Sicht des ZVEI	Es ist sicherzustellen, dass es zwischen der delegierten Verordnung (EU)2022/30 unter der Funkanlagenrichtlinie und dem CRA zu keiner Parallelanwendung kommt. Aus Sicht des ZVEI muss die delegierte Verordnung zurückgezogen werden, sobald der CRA in Kraft tritt. Dabei ist zu prüfen, wie eine Übergangsfrist gestaltet werden kann, um einerseits Stichtagsregelungen und andererseits Doppelanforderungen zu vermeiden. Der ZVEI fordert deshalb, dass Vorgaben aus Erwägungsgrund 30 des CRA zeitnah umgesetzt werden. Dort ist festgelegt, dass die Anforderungen aus dem CRA im Einklang stehen mit den Anforderungen der Delegierten Verordnung (EU) 2022/30 unter der RED.

	Die Normungsarbeit im Rahmen der delegierten Verordnung (EU) 2022/30 soll für den CRA übernommen werden. Für den Übergang bis zur Anwendung des CRA ist die EU-Kommission gehalten, im Rahmen eines Leitfadens auszuarbeiten, wie für Produkte unter beiden Rechtsakten die Konformität mit den jeweiligen Anforderungen bewertet werden kann.	
Betreffende Rechtsnormen	**<u>CRA</u>** **Art. 2** (1) This Regulation applies to products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network. **Art. 3** For the purposes of this Regulation, the following definitions apply: (1) 'product with digital elements' means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;	**<u>RED del. Reg. EU 2022/30</u>** **Art.1** (1) Die grundlegende Anforderung nach Artikel 3 Absatz 3 Buchstabe d der Richtlinie 2014/53/EU gilt für alle Funkanlagen, die selbst über das Internet kommunizieren können, unabhängig davon, ob sie direkt oder über andere Geräte kommunizieren („mit dem Internet verbundene Funkanlagen"). (2) Die grundlegende Anforderung nach Artikel 3 Absatz 3 Buchstabe e der Richtlinie 2014/53/EU gilt für die folgenden Funkanlagen, sofern diese Funkanlagen im Sinne von Artikel 4 Absatz 2 der Verordnung (EU) 2016/679 personenbezogene Daten im Sinne von Artikel 4 Absatz 1 der Verordnung (EU) 2016/679 oder Verkehrsdaten und Standortdaten im Sinne von Artikel 2 Buchstaben b und c der Richtlinie 2002/58/EG verarbeiten können: a) mit dem Internet verbundene Funkanlagen, die nicht unter den Buchstaben b, c oder d genannt sind, b) Funkanlagen, die ausschließlich für die Kinderbetreuung konzipiert oder bestimmt sind, c) Funkanlagen, die unter die Richtlinie 2009/48/EG fallen, d) Funkanlagen, die ausschließlich oder nicht ausschließlich dazu konzipiert oder bestimmt sind, an Folgendem getragen, festgeschnallt oder befestigt zu werden: i) einem Teil des menschlichen Körpers, einschließlich Kopf, Hals, Rumpf, Arme, Hände, Beine und Füße, ii) oder an von Menschen getragenen Kleidungsstücken, einschließlich Kopfbedeckungen, Handschuhen und Schuhen. (3) Die grundlegende Anforderung nach Artikel 3 Absatz 3 Buchstabe f der Richtlinie 2014/53/EU gilt für alle mit dem Internet verbundenen Funkanlagen, wenn diese dem Besitzer oder Nutzer ermöglichen, Geld, monetäre Werte oder virtuelle Währungen im

		Sinne von Artikel 2 Buchstabe d der Richtlinie (EU) 2019/713 zu übertragen.

AI Act vs. Maschinen-Verordnung

<table>
<tr><td>Zielkonflikt</td><td colspan="2">Abweichende Definition „Sicherheitsbauteil“

In der Maschinen-VO wird ein Sicherheitsbauteil als eine Komponente betrachtet, die separat in Verkehr gebracht wird. Die Sicherheitskomponente ist in der Maschinen-VO eine zusätzliche Sicherheitsvorrichtung, die auf die eigentliche Funktion der Maschine nur dann Auswirkung hat, wenn sich ein Sicherheitsvorfall ereignet hat. Die Maschine wäre auch ohne dieses Sicherheitsbauteil voll funktionsfähig. Gem. der Definition in der Maschinen-VO ist ein Sicherheitsbauteil „zur Gewährleistung einer Sicherheitsfunktion konstruiert oder bestimmt <u>und</u> dessen Ausfall oder Fehlfunktion die Sicherheit von Personen gefährdet, die aber für das Funktionieren dieses Produkts nicht erforderlich ist“

Im Sinne des AI Act hingegen ist ein Sicherheitsbauteil immer ein „Bestandteil eines Produktes oder KI-Systems“ und wird demnach nicht separat in Verkehr gebracht. Es ist somit auch nicht losgelöst von der Maschine zu betrachten, wie es bei der Maschinen-VO der Fall ist. Ein Sicherheitsbauteil gem. AI Act ist dadurch definiert, dass es „eine Sicherheitsfunktion für dieses Produkt oder KI-System erfüllt <u>oder</u> dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Eigentum gefährdet“. Zudem sind in der Definition eines Sicherheitsbauteils gemäß AI Act solche möglichen Fehlfunktionen enthalten, die nicht nur die Sicherheit („health and safety of persons“), sondern auch Eigentum („property“) betreffen. Die Ausweitung der Definition auf Eigentumsschäden erhöht die Anzahl der Produkte, die als Sicherheitskomponenten definiert werden, erheblich. Dies kann auch zu einer deutlich größeren Zahl jener Produkte führen, die unnötigerweise auch als Hochrisikosysteme bewertet werden könnten. Der AI Act bleibt hier undeutlich.

Insgesamt jedoch ist die Definition von Sicherheitsbauteilen unter dem AI-Act deutlich weiter gefasst als in der Maschinen-VO. Durch die inkonsistenten Definitionen des Sicherheitsbauteils kann es dazu führen, dass bei einem Produkt eine verbaute Komponente nach AI Act als Sicherheitskomponente klassifiziert wird und nach der Maschinen-VO nicht.</td></tr>
<tr><td>Bewertung und Empfehlung aus Sicht des ZVEI</td><td colspan="2">In den Guidance-Dokumenten zum AI Act muss klargestellt werden, dass bei Sicherheitsbauteilen, die auch unter die Maschinen-VO fallen, die Definition der Maschinen-VO ausschlaggebend dafür ist, ob die Anwendung als Hochrisiko-KI eingestuft wird oder nicht.</td></tr>
<tr><td>Betreffende Rechtsnormen</td><td><u>AI Act</u>

Art. 3
(14) „Sicherheitsbauteil“ einen Bestandteil eines Produkts oder KI-Systems, der eine Sicherheitsfunktion für dieses Produkt oder KI-System erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Eigentum gefährdet;</td><td><u>Maschinen-VO</u>

Art. 3
3. „Sicherheitsbauteil “ bezeichnet ein physisches oder digitales Bauteil, einschließlich Software, eines in den Anwendungsbereich dieser Verordnung fallenden Produkts, die zur Gewährleistung einer Sicherheitsfunktion konstruiert oder bestimmt ist, gesondert in Verkehr gebracht wird und dessen Ausfall oder Fehlfunktion die Sicherheit von Personen gefährdet, die aber für das Funktionieren dieses Produkts nicht erforderlich ist oder durch normale Bauteile ersetzt werden kann, um den Betrieb dieser Produkte zu gewährleisten;</td></tr>
</table>

Data Act vs. DSGVO

Zielkonflikt	**Herausforderungen im Umgang mit Mischdatensätzen** Insofern der Nutzer nicht auch die betroffene Person ist, deren Daten verlangt werden, verweisen Art. 4 Abs. 12 und Art. 5 Abs. 7 Data Act darauf, dass für die Übermittlung personenbezogener Daten eine Rechtsgrundlage nach Art. 6 und ggf. Art. 9 DSGVO vorliegen müsse. Dabei ist zu beachten, dass der Data Act selbst keine Rechtsgrundlage zur Verarbeitung von personenbezogenen Daten (gem. Art. 6 Abs 1 lit. DSGVO) darstellt. Vielmehr wird wie beschrieben, schlicht auf die generellen Befugnisnormen der DSGVO aus Art. 6 und 9 DSGVO verwiesen. Der Dateninhaber kommt hierdurch in die missliche Situation, dass bei Datenzugangsersuchen durch den Nutzer, Teile eines Mischdatensatzes Personenbezug zum Nutzer, andere Teile Personenbezug zu etwaigen Dritten und wieder andere Teile gar keinen Personenbezug haben können. Eine Rechtsgrundlage nach Art. 6 oder 9 DSGVO (in aller Regel wird dies eine Einwilligung des ersuchenden Nutzers sein) kann sich in diesem Fall nur auf den Datensatzteil beziehen, der Personenbezug zum Nutzer aufweist. Für Datensatzteile mit Personenbezug zu Dritten müssten jeweils gesonderte Einwilligungen eingeholt oder sie müssten ausgesondert werden. Hier ergeben sich in der Praxis Abgrenzungsschwierigkeiten. Insbesondere in Mehrpersonenverhältnissen, wie beispielweise bei der gemeinsamen Nutzung einer Kaffeemaschine im Büro, liegen regelmäßig umfangreiche Mischdatensätze vor, die faktisch oft nur schwer trennbar sind. Die eindeutige Zuordnung des Datenteils mit Personenbezug zum Datensubjekt oder zu Dritten ist technisch nicht oder nur durch unverhältnismäßig großen Aufwand realisierbar. Hier hilft auch Erwägungsgrund 35 des Data Acts, der von “technisch machbar” spricht nur bedingt weiter, da eine eindeutige Definition, die festlegt was unter “technisch machbar” zu verstehen ist, vollends fehlt. Auch der Hinweis in Erwägungsgrund 7 des Data Acts, der Dateninhaber könne dem Datenzugangsverlangen unter anderem nachkommen, indem er personenbezogene Daten anonymisiert, hilft auch nicht weiter. Zum einen ergibt sich auch hier das Problem der schweren Trennbarkeit von Mischdatensätzen; im Ergebnis müsste der Dateninhaber bestimmte ermittelte Datensatzteile anonymisieren. Zum anderen besteht auch in Bezug auf die Anonymisierung im Rahmen der DSGVO selbst eine große Unklarheit und keine eindeutige Gesetzeslage.
Bewertung und Empfehlung aus Sicht des ZVEI	Der Schutz personenbezogener Daten sowie das Recht des Einzelnen auf informationelle Selbstbestimmung sind hoch anzusiedeln und müssen garantiert bleiben. Gleichwohl ist der Austausch und die Nutzung von Daten für die deutsche und europäische Wirtschaft – insbesondere die datengetriebene Elektro- und Digitalindustrie – essenziell, um neue Technologien und Innovationen in den Markt zu bringen und damit für eine nachhaltige Wertschöpfung zu sorgen. Vor diesem Hintergrund plädieren wir für einen „ermöglichenden“ Datenschutz und regen an, das grundsätzliche Verbotsprinzip der DSGVO zu überwinden. Zumindest jedoch müssen dringend die Erlaubnistatbestände so angepasst und ausgeweitet werden, dass die Verarbeitung von personenbezogenen Daten nicht mehr im Widerspruch zu den Zielen einer datengetriebenen Wirtschaft und den Vorgaben aus dem Data Act stehen. Im konkreten Fall könnte dies erreicht werden, wenn der Data Act selbst als Erlaubnistatbestand i.S.d. Art. 6 Abs. 1 lit c DSGVO. angesehen werden würde. Darüber hinaus müsste in Bezug auf die Anonymisierung personenbezogener Daten im Rahmen der DSGVO klargestellt werden, dass der Anonymisierung ein relatives Verständnis zugrunde liegt, also dass eine Anonymisierung auch dann vorliegt, wenn eine Re-Identifizierbarkeit der betroffenen Person nicht gänzlich ausgeschlossen ist aber aufgrund eines unverhältnismäßig hohen Aufwands ausscheidet.

Betreffende Rechtsnormen	**<u>Data Act</u>** **Art. 4** (5) Um zu überprüfen, ob eine natürliche oder juristische Person als Nutzer für die Zwecke von Absatz 1 einzustufen ist, verlangt der Dateninhaber von dieser Person keine Informationen, die über das erforderliche Maß hinausgehen. Dateninhaber bewahren keine Informationen über den Zugang des Nutzers zu den verlangten Daten – insbesondere keine Protokolldaten – auf, die über das hinausgehen, was für die ordnungsgemäße Ausführung des Zugangsverlangens des Nutzers und für die Sicherheit und Pflege der Dateninfrastruktur erforderlich ist. **Art. 5** (6) Der Dateninhaber darf ohne Weiteres verfügbare Daten nicht verwenden, um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Dritten oder in die Nutzung durch den Dritten auf jegliche andere Art, die die gewerbliche Position des Dritten auf den Märkten, auf denen dieser tätig ist, untergraben könnte, zu erlangen, es sei denn, der Dritte hat eine solche Nutzung genehmigt und hat die technische Möglichkeit, diese Genehmigung jederzeit einfach zu widerrufen.	**<u>DSGVO</u>** **Art. 6** (1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: (a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben; (b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen; (c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt; (f) die Verarbeitung ist zur Wahrung der berechtigten Interessen Des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. **Art. 9** (1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt. (2) Absatz 1 gilt nicht in folgenden Fällen: (a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,

		(b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,

Datum: 10.09.2024

Kontakt

Jochen Reinschmidt • Bereichsleiter Digitalisierung & Recht •
Tel.: +49 30 306960 23 • Mobil: +49 174 9414 164 • E-Mail: Jochen.Reinschmidt@zvei.org

ZVEI e. V. • Verband der Elektro- und Digitalindustrie • Charlottenstraße 35/36 • 10117 Berlin
Lobbyregisternr.: R002101 • EU Transparenzregister ID: 94770746469-09 • www.zvei.org