Position der Software AG zum Data Act-E der EU-Kommission

Version 3.0 | 02. 06. 2022

software AG

Management Summary

- Der Data Act bietet aus Sicht der Software AG die Chance, eine von europäischen Werten geleitete offene und demokratische Datenwirtschaft zu gestalten. In seiner jetzigen Form kann der Data Act allerdings sehr weit ausgelegt werden und nicht intendierte Kollateralschäden nach sich ziehen. Es fehlt insbesondere an klaren Definitionen und Eingrenzungen der Anwendungsfelder. Für Unternehmen bedeutet dies zusätzliche Rechtsunsicherheiten beim Umgang mit Daten. In Verbindung mit dem durch die Anforderungen zusätzlich notwendigen technischen Aufwand könnte dies Unternehmen davon abhalten, in die Erhebung von Daten und die Entwicklung eigener IoT-Services zu investieren.
- Besonders kritisch sehen wir die in Kapitel 6 vorgesehenen Regelungen zum Wechsel zwischen Anbietern von Datenverarbeitungsdiensten („data processing service provider“). Die vorgeschlagenen Regelungen zum Switching gehen an vielen Stellen sowohl über das technisch Machbare als auch über das wirtschaftlich Sinnvolle hinaus. Grundsätzlich sollte bei Festlegung der Anforderungen nach den jeweiligen Cloud-Schichten (IaaS, PaaS, SaaS) differenziert werden, da sich die technischen und wirtschaftlichen Herausforderungen jeweils deutlich unterscheiden können. Solch eine Differenzierung wird zwar ansatzweise in Artikel 26 vorgenommen, sollte jedoch ausgebaut werden und z.B. auch für die Kündigungsfristen gelten.
- Technologische Unterschiede werden in Kapitel 6 des Data Acts nicht ausreichend berücksichtigt. Datenverarbeitungsdienste – auch wenn sie die gleiche Funktion erfüllen – werden in der Regel auf unterschiedlichste Weise realisiert, zum Beispiel in Hinblick Datenformate, Datensemantiken, Ausführungsumgebungen, Funktionslogiken oder interne IT-Architekturen. Jeder dieser Unterschiede stellt ein potenzielles Hindernis dar. All diese Hindernisse zu beseitigen, würde Unternehmen vor große wirtschaftliche und technische Herausforderungen stellen. Vor diesem Hintergrund sollte genauer definiert werden, was unter einem technischen Hindernis zu verstehen ist, welche Elemente der IT-Architektur diese betreffen und wie weit die unterstützenden Maßnahmen seitens des ursprünglichen Diensteanbieters gehen müssen, um einen Wechsel zu ermöglichen.
- Die im Data Act-E (Art. 23) vorgesehene maximale Kündigungsfrist von 30 Tagen für die Portierung zu einem anderen Anbieter schränkt die Vertragsfreiheit unnötig ein. In der Praxis würde dies bedeuten, dass Diensteanbieter keine Rabatte auf langfristige Verträge gewähren könnten. Dies würde die Kosten für sämtliche Kunden – auch für diejenige, die langfristige Vertragsbeziehungen eingehen möchten - unnötig und dramatisch erhöhen und die Entwicklung von Partnerschaften, Datenräumen oder anderen Formen von Daten-Ökosystemen stark einschränken.

Grundsätzliche Anmerkungen

Die EU-Kommission hat mit ihrem Entwurf zum Data Act (Data Act-E) weitreichende Regelungen für den Zugang und die Verwendung von nicht-personenbezogenen Daten in der EU vorgelegt, mit dem Ziel, Industriedaten in Europa zu erschließen, die Unternehmen, Verbrauchern, öffentlichen Diensten und der Gesellschaft insgesamt zugutekommen sollen. Die Software AG begrüßt dieses Vorhaben. Aus unserer Sicht bietet der Data Act als horizontale Regulierung – sofern richtig gemacht – die Chance, eine von europäischen Werten geleitete offene und demokratische Datenwirtschaft zu gestalten, in der es eine faire Verteilung zwischen den an der Wertschöpfung Beteiligten gibt.

Allerdings drängt sich uns der Eindruck auf, dass im Vorfeld des Data Acts keine Problemanalyse betrieben worden wäre, die seiner fundamentalen Bedeutung ausreichend Rechnung trägt. Insbesondere die Gesetzesbegründung der Kommission beruht in weiten Teilen auf – zwar wohlbegründeten und nachvollziehbaren – Annahmen, es fehlt jedoch die empirische Evidenz. Ohne diese steht der Data Act auf tönernen Füßen. Zudem ist unseres Erachtens nach den komplexen Auswirkungen – und vor allem Nebenwirkungen – des Data Acts noch nicht angemessen Rechnung getragen worden. Schwere Kollateralschäden – als horizontale Regulierung wirkt der Data Act quer durch alle Branchen uns Sektoren – sind deshalb unvermeidlich.

So haben wir die große Sorge, dass der Data Act in seiner jetzigen Form mit unnötigen Aufwänden, Kosten und Rechtsunsicherheiten für die Unternehmen verbunden ist. Sie bergen die Gefahr, Unternehmen davon abzuschrecken, in die Entwicklung von IoT-Produkten und Services zu investieren. In der Folge würde Europa eher früher als später seine Wettbewerbsfähigkeit verlieren. Um dies zu verhindern, möchte sich die Software AG mit konkrete Vorschläge in die politische Debatte um den Data Act einbringen und Möglichkeiten aufzeigen, wie sich einerseits die – richtigen und wichtigen – Ziele der EU-Kommission erreichen lassen und dabei andererseits die negativen (nichtintendierten) Folgen minimiert werden können.

Besonders die in Kapitel 6 vorgesehenen Regelungen zum Wechsel zwischen Anbietern von Datenverarbeitungsdiensten („data processing service provider“) sehen wir mit größter Sorge. Wir unterstützen zwar das Ziel der EU-Kommission, den Wechsel zwischen Diensteanbietern durch den Abbau von Lock-ins zu erleichtern und damit den Wettbewerb in Europa zu stärken. Allerdings gehen die vorgeschlagenen Regelungen zum Switching an vielen Stellen sowohl über das technisch Machbare als auch über das wirtschaftlich Sinnvolle hinaus: Dies gilt insbesondere für die:

- Kündigungsfrist von maximal 30 Tagen
- Mitnahme **aller** Daten, Applikationen und Data Assets zum neuen Anbieter
- Speicherung und Übergabe **aller** bei der Nutzung des Dienstes anfallenden Daten

- Sicherstellung der funktionalen Äquivalenz durch den alten Anbieter
- Verpflichtung, die Dienste innerhalb von 30 Tagen On-Premise lauffähig zu machen

Diese Regelungen sind derart weitreichend bzw. wären – sofern überhaupt – nur unter solch enormen technischen Aufwand zu realisieren, dass es zum einen für europäische Unternehmen unattraktiver wird, eigene Cloud- und Edge-Services zu entwickeln. Zum anderen würde die Umsetzung der vorgeschlagenen Regelungen, die Preise für Datenverarbeitungsdienste drastisch erhöhen, insbesondere durch die Auflage, ***alle*** während ihrer Nutzung angefallenen Daten zu speichern und beim Anbieterwechsel dem neuen Anbieter zu übermitteln. Vielen Anwendungen würde dadurch ungewollt der wirtschaftliche Boden entzogen, wodurch Europa bei der Nutzung von Datenverarbeitungsdiensten weiter ins Hintertreffen geriete. Damit würde zugleich die industrielle Entwicklung der letzten Jahren zunichte gemacht werden. Vor allem im B2B-Bereich haben zahlreiche Unternehmen damit begonnen, in den noch jungen Markt zu investieren. Sie müssten nicht nur befürchten, dass ihre Kunden innerhalb von 30 Tagen zu einem anderen Anbieter wechseln, sondern zusätzlich Ressourcen aufwenden, um diesen Wechsel technisch zu ermöglichen. Die hiermit verbundenen Unsicherheiten in Hinblick auf die Zukunftsfähigkeit von eigenen Technologien und Geschäftsmodellen können etablierte und große Cloud-Anbieter wesentlich leichter abfangen. Dies würde die Datengravitation hin zu den größeren Cloud-Anbietern erhöhen und schlussendlich dazu führen, dass kleinere Anbieter branchenspezifischer Cloud-Dienste von größeren Unternehmen aus dem Markt gedrängt werden.

Um diese Kollateralschäden zu mindern und für einen fairen Interessensausgleich zu sorgen, schlagen wir –folgende Änderungen am Data Act E vor:

Kapitel 1 – “General Provisions”

Den Begriff „service model“ definieren (Art. 2, Nr. 13)

Ein grundsätzliches Problem des Data Act-E besteht aus Sicht der Software AG darin, dass viele wichtige Begriffe entweder nur unzureichend oder gar nicht definiert werden. Der Data Act-E lässt erheblichen Unklarheiten über den Anwendungsbereich der Regelungen. Dies betrifft insbesondere die Regelungen zum Wechsel zwischen Datenverarbeitungsdienste. So wird der Begriff „service model“ nicht definiert, obwohl er für die Definition des „service type“ im Data Act eine zentrale Bedeutung einnimmt. Da auch im IT-Bereich keine einheitliche Definition des Begriffs „service model“ existiert, kann er sogar soweit ausgelegt werden, dass er geschäftsmodellabhängige Servicekonfiguration umfasst (wie im ITIL-Standard für IT-Infrastrukturdienste).

Kapitel 2 – “Business to consumer and business to business data sharing”

Horizontale Regulierung auf ein Mindestmaß beschränken und Fokus auf sektorspezifische Regulierung legen (Art. 3 – 7)

Die im Data Act-E Kapitel 2 vorgesehenen Datenzugangsrechte könnten unerwünschte industriepolitische Konsequenzen nach sich ziehen. So dürfen die vom Data bereitgestellten Daten zwar nicht für die Entwicklung von Konkurrenzprodukten genutzt werden, datenbasierte Dienste sind von diesem Wettbewerbsverbot jedoch bewusst ausgenommen. Wir können das Ansinnen der Kommission nachvollziehen, mit dieser Regelung After-Sales-Market zu stärken, sehen zugleich allerdings die Gefahr, dass dies ungewollt zu Wettbewerb an anderer Stelle führt: In der Industrie ist zu beobachten, dass sich die Wertschöpfung immer stärker von der Herstellung eines Produktes hin zu Services rund um das Produkt verlagert. Bisher konnten sich die produzierenden Unternehmen den Vorteil zu Nutze machen, den Zugang zu den Industriedaten zu besetzen und auf deren Basis innovative digitale Services zu entwickeln. Dieser Vorteil würde durch die im Data Act-E vorgesehenen Datenzugangsrechte erheblich geschwächt. Dies ist vor allem deshalb kritisch, da digitale Services mehr und mehr ins Zentrum des Leistungs- und Wertversprechens rücken. Vereinfacht ausgedrückt: Für den Kunden wird es irrelevant, ob er eine Maschine von Hersteller A oder Hersteller B kauft, Hauptsache der digitale Service X läuft auf ihr. Die Maschine wäre dann nur noch der physische und austauschbare Träger für die digitalen Services – mit den entsprechenden Implikationen für die Wertschöpfungsverteilung. In Anbetracht dieser industriepolitischen Überlegungen sollten die Gesetzgeber in Erwägung ziehen, horizontal nur absolute Mindestanforderungen zu formulieren und – falls notwendig – weitergehende Anforderungen über problemlösungsorientierte und sektorspezifische Datenzugangsregeln festzulegen. Es sollte vor allem nicht dazu kommen, dass der Data Act in ein bereits funktionierendes System eingreift. Im Industrie 4.0-Umfeld zum Beispiel, können Fragen des Datenzugangs bereits über Verträge flexibel und für alle Parteien fair gelöst werden.

Der Data Act würde im Zweifel neue Rechtsunsicherheiten, Schwachstellen im Schutz von Geschäftsgeheimnissen und bürokratische Hürden schaffen, die Unternehmen daran hindern, in innovative Geschäftsmodelle auf Basis des eigenen Datenschatzes zu investieren. Um diese ungewollten Effekte zu verhindern, muss der Data Holder seine in den zu bereitzustellenden Daten enthaltenen Geschäftsgeheimnisse unbedingt für sich behalten können und nicht – wie im aktuellen Entwurf des Data Acts vorgesehen – in letzter Konsequenz preisgeben müssen, wenn sie sich nicht aus den Daten entfernen lassen. Gleichwohl dürfen nicht alle Daten vom Data Holder als Geschäftsgeheimnis deklariert werden, um damit die Datenbereitstellung zu

unterbinden. Deshalb sollte im Data Act zudem konkretisiert werden, was Geschäftsgeheimnisse im Sinne der Verordnung sind.

Darüber hinaus ist uns unklar, welche Entschädigungsansprüche der Data Holder gegenüber dem Data Recipient im Falle der widerrechtlichen Datennutzung hat, also wenn z.B. die bereitgestellten Daten doch zur Entwicklung eines Konkurrenzproduktes verwendet werden. So ist im Entwurf des Data Acts zwar vorgesehen, dass der Data Holder technische Vorkehrungen gegen die missbräuchliche Datennutzung treffen und bei Zuwiderhandlung vom Data Recipient sowohl die Zerstörung der Daten als auch die Entfernung der auf ihnen basierenden Daten, Produkten und Services vom Markt verlangen darf. Über die neuralgische Frage, ob der Data Holder auch Entschädigungsansprüche für entgangene Umsätze hat, darüber schweigt er sich jedoch aus. Hier sollte unserer Meinung nach der Data Act als horizontale Regelung um ein dezidiertes Haftungsregime nachgebessert werden, um die faire Wertschöpfungsverteilung abzusichern.

Rechtsunsicherheiten bei der Anonymisierung und Pseudonymisierung personenbezogener Daten adressieren (Art. 3 - 7)
In der Unternehmenspraxis gibt es große Unsicherheit hinsichtlich der Trennung von personenbezogenen und nicht-personenbezogenen Daten. Laut einer Studie des IW Köln bezeichnen 85 Prozent der befragten Unternehmen „datenschutzrechtliche Grauzonen" als Hemmnis für die wirtschaftliche Nutzung von Daten.[1] Der Data Act sollte dieses Problem zu adressieren. Durch die Regelungen drohen neue Rechtsunsicherheiten und Abgrenzungsschwierigkeiten zwischen personenbezogenen und nicht-personenbezogenen Daten. Besonders dringend sollte in diesem Zusammenhang geklärt werden, wann personenbezogene Daten als rechtssicher anonymisiert gelten.

Kapitel 6 – „Switching between data processing services"

Anwendungsbereich für die Portierung von Applikationen einschränken (Art. 23 Nr. 1c)
Gemäß Art. 23 Nr. 1c müssen sämtliche Daten, Applikationen und sonstige digitale Güter eines Kunden auf einen anderen Dienstleister übertragbar sein. Da Applikationen nicht in dem Data Act-E definiert werden, ist der potenzielle Anwendungsbereich sehr weit gefasst und würde auch Applikationen miteinschließen, für die der Kunde lediglich das Nutzungsrecht hat. In einem PaaS/SaaS-Umfeld haben die Kunden in der Regel Zugang zu und das Recht auf die Nutzung von vielen verschiedenen, aber allgemeinen Funktionen wie Dashboards und Widgets, Identitäts- und Zugriffsverwaltungssysteme, Such- und Abfragemechanismen,

[1] Vgl. IW Köln (2021): Hemmnisse_der_Datenwirtschaft_Studie.pdf

Speicherfunktionen und vieles mehr. Dem ursprünglichen Diensteanbieter die Verantwortung für die Portierung all dessen auf einen anderen Diensteanbieter („target service provider“) zu übertragen, bedeutet im Grunde, dass sein gesamtes PaaS/SaaS-Angebot auf einen anderen Diensteanbieter übertragbar sein muss, unabhängig vom Recht am geistigen Eigentum und den architektonischen Unterschieden der angebotenen Dienste.

Ohnehin macht der Begriff „Applikationen“ in einer Cloud-nativen PaaS/SaaS-Umgebung oft keinen Sinn, da PaaS/SaaS-Anbieter regelmäßig keine "Applikationen" in dem Sinne bereitstellen, dass eine oder mehrere ausführbare Dateien gezielt auf einem Rechenknoten im Auftrag eines Nutzers ausgeführt werden. Stattdessen bieten alle Anbieter von Cloud-Diensten heute so genannte Fähigkeiten (capabilities) an, deren Bereitstellung auf eine verteilte und elastische Recheninfrastruktur basiert. In Bezug auf die Portierung schlagen wir vor, den Begriff "Applikationen" durch den neuen Begriff "Funktionslogik" zu ersetzen, der einen zusammenhängenden Datensatz (einschließlich aller Metadaten) meint, die das Verhalten eines Datenverarbeitungsdienstes nach ordnungsgemäßer Bereitstellung beeinflussen, ergänzen oder ändern können.

Technologische Unterschiede berücksichtigen (Art. 23ff.)

Viele der weitreichenden Regelungen für den Wechsel eines Diensteanbieters sind technisch nicht oder nur schwer realisierbar. Laut Art. 23 des Data Act-E sollen Diensteanbieter dazu verpflichtet werden, technische Hindernisse zu beseitigen und den Kunden dabei zu unterstützen, seine Daten, Applikationen und andere digitale Güter („digital assets“) zu einem anderen Diensteanbieter zu portieren. Allerdings werden Datenverarbeitungsdienste – auch wenn sie die gleiche Funktion erfüllen – in der Regel auf unterschiedlichste Weise realisiert, zum Beispiel in Hinblick Datenformate, Datensemantiken, Ausführungsumgebungen (Intel Prozessoren vs. ARM Prozessoren vs. GPUs), Funktionslogiken oder interne IT-Architekturen. Jeder dieser Unterschiede stellt ein potenzielles Hindernis dar. Soll etwa im PaaS/SaaS-Umfeld eine Applikation zu einem anderen Diensteanbieter portiert werden, reicht es nicht, das „grundlegende Datenverarbeitungsmodell“ nach Art. 2, Nr. 13 zu teilen, sondern die beiden Diensteanbieter müssten dieselbe Cloud-Architektur nutzen. Eine ähnliche Situation ergibt sich bei der in Art. 24 (a) vorgesehenen Portierung auf ein On-Premise-System. Dies ist nur dann realistisch, wenn das On-Premise-System über eine nahezu identische technische Architektur verfügt. Solch eine technische Äquivalenz zwischen Diensteanbieter herzustellen ist in der Praxis oftmals gar nicht möglich – insbesondere dann, wenn der ursprüngliche Diensteanbieter („original service provider“) die alleinige Verantwortung dafür tragen soll. Vor diesem Hintergrund sollte genauer definiert werden, was unter einem technischen Hindernis zu verstehen ist, welche Elemente der IT-Architektur diese betreffen und wie weit die unterstützenden Maßnahmen seitens des ursprünglichen Diensteanbieters gehen müssen, um einen Wechsel zu ermöglichen. In keinem Fall sollte es dazu kommen, dass Diensteanbieter ihre Architekturen aus Portabilitätsgründen an die Architektur anderer Diensteanbieter anpassen müssen. Sie sollten weiterhin die Freiheit haben, Applikationen anzubieten, die sich nicht ohne Weiteres auf andere Systeme übertragen lassen.

Maximale Kündigungsfrist verlängern (Art. 23, Nr. 1a)

Die im Data Act-E vorgesehene maximale Kündigungsfrist von 30 Tagen für die Portierung zu einem anderen Anbieter schränkt die Vertragsfreiheit unnötig ein. In der Praxis würde dies bedeuten, dass Diensteanbieter keine Rabatte auf langfristige Verträge gewähren könnten. Dies würde die Kosten für sämtliche Kunden – auch für diejenige, die langfristige Vertragsbeziehungen eingehen möchten - unnötig und dramatisch erhöhen und die Entwicklung von Partnerschaften, Datenräumen oder anderen Formen von Daten-Ökosystemen stark einschränken.

Zu portierende Datenmenge auf ein angemessenes Maß beschränken (Art. 23 Nr. 1c)

Technisch schwierig gestaltet sich zudem die Portierung von Daten. Um den Anbieter effektiv zu wechseln, ist zwar die die Portierung von Daten notwendig. In bestimmten Situationen - wie z. B. IoT/IIoT/Industrie 4.0 - kann jedoch die schiere Menge aller vom Nutzer (d. h. seinen Geräten oder Maschinen) erzeugten Daten viel zu groß sein, um vom ursprünglichen Dienstanbieter kontinuierlich gespeichert zu werden und beim Wechsel zur Verfügung zu stehen. Ein Beispiel: Windkraftanlagen eines Windparks verfügen über mehrere tausend Sensoren, die hundertmal pro Sekunde Sensormesswerte an einen zentralen Datenverarbeitungsdienst (= typischerweise eine IoT-Plattform) senden können. Typische europäische Kunden produzieren dabei etwa 20-50 TB (Terabyte) an Rohdaten pro Monat. Diese werden üblicherweise anaylsiert und ggf. aggregiert, aber nicht in der Form von Rohdaten gespeichert. Im Laufe längerer (mehrjähriger) Dienstleistungsverträge müsste der Dienstanbieter nur bedingt durch den Data Act („to port all data, applications and digital assets generated directly or indirectly by the customer „) jedoch für die gesamte Vertragslaufzeit alle diese Daten, also mehrere Petabytes (1 PB = 1.000 TB) an Nutzungsdaten speichern. Da die Kosten für die Speicherung dieser – normalerweise nicht gespeicherten - Daten im Bereich von mehreren Millionen Euro pro Jahr liegen, werden europäische Kunden von IoT-Plattformanbietern nicht in der Lage sein, mit anderen (ausländischen) Anbietern zu konkurrieren, da sie einen enormen Kostennachteil haben. Zudem erzeugt die Speicherung solcher Datenmengen einen hohen Energieaufwand, der im Sinne des Green Deal vermieden werden sollte. Die konkrete, zu portierende Menge der zu übertragenden gespeicherten Daten sollte daher – wenn nicht vertraglich anders vereinbart – auf ein angemessenes Maß beschränkt werden.

Die Anforderung nach vollständiger Kontinuität abschwächen (Art. 24 Nr. 1a)

In Art. 24 Nr. 1a wird der Diensteanbieter verpflichtet, im Rahmen des Portierungsprozess vollständige Kontinuität bei der Erbringung der jeweiligen Funktionen oder Dienste zu gewährleisten. Diese Anforderung lässt außer Acht, wie Migrationsprojekte für Daten oder Anwendungen in der Praxis funktionieren. Bei einem Migrationsprojekt gibt es entweder einen harten Schnitt und ein bestimmtes Datum bzw. eine bestimmte Uhrzeit, bei dem die Benutzer von einem Dienstanbieter zum anderen wechseln (dies ist diskontinuierlich), oder es muss eine Art Vermittlungsgateway sowohl beim ursprünglichen als auch beim zukünftigen Diensteanbieter eingesetzt werden. Je nach Stand der Migration (oder Portierung) bestimmt dieser Vermittlungsgateway dynamisch, ob eine Serviceanfrage eines Benutzers an die alte

Instanz des Dienstes beim ursprünglichen Dienstanbieter oder an die neue Instanz des Dienstes beim neuen Diensteanbieter adressiert werden soll. Dies geschieht jedoch nicht in Form einer einfachen "Umschaltung", sondern erfordert ein vollwertiges Migrationsprojekt, das von jemandem aufgesetzt und finanziert werden muss.

Frist zur Umsetzung von Interoperabilitätsanforderung einführen (Art. 26 Nr. 3)

Laut Art. 26 Nr. 3 sollen Anbieter von Datenverarbeitungsdiensten die Kompatibilität mit europäischen Interoperabilitätsstandards gewährleisten. Da es derzeit keine solchen Standards gibt, müsste jeder Diensteanbieter seine Dienste und APIs ändern, wenn ein solcher Standard in Kraft tritt. Eine solche Implementierung braucht jedoch einen stabilen Standard und ausreichend Zeit auf Seiten der Diensteanbieter, bevor diese mit der erforderlichen Sorgfaltspflicht die Konformität mit einem solchen Interoperabilitätsstandard erklären können.

Die Formulierung suggeriert jedoch, dass die Diensteanbieter sofort und unverzüglich auf einen völlig neuen (Interoperabilitäts-)Standard umzustellen müssen, sobald er in Kraft tritt. Dies kann realistischerweise nicht erreicht werden. Daher schlagen wir vor, den Diensteanbietern eine angemessene Frist für die Umsetzung einzuräumen.

Kapitel 8 – „Interoperability“

Datenräume mit mehreren Betreibern berücksichtigen (Art. 28)

Die derzeitige Formulierung der Anforderungen an Datenräume scheint sich zu sehr auf Datenräume zu konzentrieren, die von einem einzigen Betreiber betrieben werden und der die alleinige Verpflichtung hätte, die Anforderungen zu erfüllen. Abgesehen davon, dass der Begriff "Betreiber" im Data Act-E nicht definiert wird, entspricht diese Begrenzung nicht dem derzeitigen Aufbau vieler Datenräume. Diese bestehen in der Regel aus einer verwaltenden Einrichtung, die den eigentlichen Betrieb der Ökosystemdienste (z. B. Identitäts- und Zugriffsmanagementdienste, Katalogdienste, Vokabeldrehkreuzdienste, Vertrauensankerdienste usw.) an einen Dritten (manchmal als technischer Betreiber des Datenraums bezeichnet) überträgt. In einem solch typischen Aufbau, sollte – wenn überhaupt – die verwaltende Einrichtung verantwortlich sein. Der Vorschlag berücksichtigt auch keine föderierten (d. h. es gibt mehr als einen Betreiber) oder dezentralisierten Datenräume (d. h. es kann keine Gruppe von Betreibern ermittelt werden).

Keine Konformitätserklärung für smart contracts einführen (Art. 30, Nr. 2)

Der Gesetzgeber sollte von einer EU-Konformitätserklärung absehen. Keine andere Art von Software muss eine solche Erklärung abgeben (nicht einmal eingebettete Systeme für autonomes Fahren oder KI/ML-Anwendungen), und die bestehenden Gesetze zur Produktsicherheit und zum Deliktsrecht reichen aus.