Centrum für Europäische Politik
FREIBURG | BERLIN

cepInput

Nr. 18 | 2024 19. Dezember 2024

EU-Cloud-Zertifizierung in der Sackgasse

(Aus-)Wege hin zu einer resilienten Cloud-Politik in der EU

Philipp Eckhardt und Anja Hoffmann

Seit Jahren wird über die Etablierung eines EU-Schemas zur Zertifizierung der Cybersicherheit von Cloud-Diensten (EUCS) diskutiert. Debatten rund um die Einbeziehung sogenannter Souveränitätsanforderungen in ein EUCS verzögern jedoch eine Einigung. Solche Anforderungen sollen die Cybersicherheit der Cloud-Dienste stärken. Sie könnten es jedoch Cloud-Nutzern in der EU erschweren, auf Cloud-Dienste aus Drittstaaten zurückzugreifen. Dieser cepInput skizziert (Aus-)Wege aus der in eine Sackgasse geratenen Diskussion um das EUCS und zeigt Vorschläge für eine resiliente EU-Cloud-Politik auf. Die Zeit drängt, denn die Cloud-Infrastruktur ist digital- und sicherheitspolitisch von enormer Bedeutung.

- Ein EUCS kann, bei adäquater Ausgestaltung, den Markt für cybersichere Cloud-Dienste beleben und das Vertrauen potenzieller Nutzer in solche Dienste stärken. Auch die Förderung von cybersicheren Cloud-Diensten, die gleichzeitig die digitale Souveränität der EU unterstützen, erscheint aus geo- und sicherheitspolitischer Perspektive nachvollziehbar. Ein EUCS, welches Souveränitätsanforderungen enthalten würde, wäre jedoch aus ökonomischer Sicht nicht nur mit Vorteilen, sondern auch mit einigen Nachteilen behaftet, und aus juristischer Sicht problematisch.
- Die Kommission sollte den EU-Rechtsakt zur Cybersicherheit (CSA), die Richtlinie zur Netz- und Informationssicherheit (NIS-2) und die EU-Vorschriften zur öffentlichen Auftragsvergabe gezielt anpassen, um eine resiliente EU-Cloud-Politik zu etablieren. Bis zum Geltungsbeginn der angepassten Regelungen sollte die Kommission – als Brückenlösung – Leitlinien für „souveräne“ Cloud-Dienste und zur Transparenz über die Eigenschaften solcher Cloud-Dienste erarbeiten und beschließen.

Inhaltsverzeichnis

1 Einleitung

In seinem im September 2024 veröffentlichten Bericht zur Zukunft der europäischen Wettbewerbsfähigkeit stellte Mario Draghi, ehemaliger Ministerpräsident Italiens und Präsident der Europäischen Zentralbank (EZB), ernüchternd fest: „Der EU-Markt für Cloud-Dienste ist weitgehend an US-amerikanische Anbieter verloren“ und „der Wettbewerbsnachteil der EU wird sich auf dem Cloud-Markt wahrscheinlich noch verstärken“. Nach Angaben der Synergy Research Group decken allein die drei als „Hyperscaler“ bezeichneten Cloud-Dienste-Anbieter Amazon Web Services, Microsoft Azure und Google Cloud mittlerweile 65% des EU-Marktes ab. Ihre weltweiten Marktanteile lagen im 2. Quartal 2024 bei zusammen 67% (32%, 23% und 12%). Gleichzeitig sinkt der Marktanteil von Anbietern aus der EU stetig, und das in einem stetig wachsenden Markt, der ein Volumen von 200 Mrd. Euro erreichen soll (2022: ca. 87 Mrd. Euro).[1,2,3] So sollen nach Analysen bis 2025 mehr als die Hälfte der IT-Ausgaben von Unternehmen in Cloud-Investitionen fließen und damit mehr als in traditionelle IT.[4,5]

Bereits im Jahr 2020 verwies die EU-Kommission in ihrer EU-Datenstrategie[6] darauf, dass Cloud-Infrastrukturen und -Dienste aus ihrer Sicht unerlässlich für den digitalen Umbau der EU-Wirtschaft seien und mahnte an, dass „die EU ihre technologische Abhängigkeit bei solchen strategischen Infrastrukturen […] verringern“ muss. Sie monierte insbesondere, dass diese Abhängigkeit die EU „anfällig gegenüber Bedrohungen von außen“ mache, dass ein Drittland über einen Anbieter des Drittlands, welcher in der EU tätig ist, unerwünschten Zugriff auf Daten von EU-Bürgern und -Unternehmen erhalten könnte, und dass berechtigte Bedenken hinsichtlich der Anwendung bzw. Anwendbarkeit ausländischer Rechtsvorschriften bei EU-Unternehmen, -Bürgern und -Behörden entstünden. Auch stellte sie fest, dass Unsicherheiten dahingehend bestünden, ob Cloud-Dienste-Anbieter aus Drittstaaten die EU-Vorschriften und -Standards auch tatsächlich beachteten.[7] Auch das „Gremium europäischer Regulierungsstellen für elektronische Kommunikation (GEREK)“ hebt in einem Bericht vom April 2024 hervor, dass „das Fehlen gleichwertiger europäischer Lösungen […] erhebliche Risiken für die digitale Transformation der industriellen Ökosysteme in der EU“ birgt, etwa im Hinblick auf mögliche Unterbrechungen der Cloud-Dienste aus Drittstaaten, bestehende Lock-in-Effekte sowie bezüglich des unrechtmäßigen Zugangs zu Daten.[8][9]

---

1 EU-Kommission (2024a), The future of European competitiveness, Part B: In-depth analysis and recommendations, Report by Mario Draghi, September 2024, S. 77.

2 Synergy Research Group (2024), Cloud Market Growth Stays Strong in Q2, While Amazon, Google and Oracle Nudge Higher, RENO, NV, 1. August 2024, siehe hier.

3 Das Gremium europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) verweist hier etwa auf erhebliche Marktzutrittsschranken, da die Bereitstellung von Cloud-Diensten erhebliche Infrastrukturinvestitionen, in IT-Ressourcen und Fachpersonal verlangt. Auch sei der Sektor „durch erhebliche versunkene Kosten, Größen- und Verbundvorteile sowie Ökosystemeffekte“ geprägt [GEREK (2024), BEREC Report on Cloud and Edge Computing Services, BoR (24) 52, 7. März 2024]. Der Bericht von Mario Draghi verweist zudem auf die vergleichsweise hohen Immobilien- und Energiekosten in der EU als Barriere für in der EU ansässige Anbieter [EU Kommission (2024a)].

4 Gartner (2022), Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025, 9. Februar 2022.

5 GEREK (2024).

6 EU-Kommission (2020a), Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, COM(2020) 66, Eine europäische Datenstrategie, 19. Februar 2020.

7 EU-Kommission (2020), S. 10.

8 EU-Kommission (2022), SWD(2022) 41, Commission Staff Working Document, EU strategic dependencies and capacities: second stage of in-depth reviews, 22. Februar 2022.

9 Der Europäische Rat forderte die Kommission in seiner „Erklärung von Budapest“ bis Juni 2025 Vorschläge zur „Stärkung der technologischen Fähigkeiten der EU“ vorzulegen und die Chancen der Datenwirtschaft zu nutzen „bei gleichzeitiger

Die enorme Abhängigkeit von Cloud-Dienste-Anbietern aus Drittstaaten und insbesondere von den US-Hyperscalern hat daher in den vergangenen Jahren die Rufe laut werden lassen, wonach die EU ihre „digitale Souveränität“ im Bereich des Cloud Computing stärken müsse. Diese Diskussion hat spätestens im Jahr 2023 auch Eingang in die Diskussion rund um die Etablierung eines Europäischen Schemas zur Zertifizierung der Cybersicherheit von Cloud-Diensten (EUCS) gefunden, als Anforderungen in dieses EUCS integriert werden sollten, die den Einsatz von Cloud-Diensten aus Drittstaaten potenziell beschränkt hätten.

In diesem cep**Input** soll in einem ersten Schritt die kontrovers geführte Debatte rund um das EUCS näher beleuchtet werden, bevor in einem zweiten Schritt Ideen für eine künftige resiliente EU-Cloud-Politik entwickelt werden. In Kapitel 2 werden zunächst die wesentlichen Vorgaben der EU-Verordnung zur Cybersicherheit (EU Cybersecurity Act, CSA)[10] erläutert. Sodann wird in Kapitel 3 genauer auf das sich in der Entwicklung befindliche EU-Schema zur Zertifizierung der Cybersicherheit von Cloud-Diensten (EUCS) eingegangen, vor allem auf die Diskussion rund um die Einfügung sogenannter Souveränitätsanforderungen in ein solches Schema. Dabei wird auch untersucht, was ein solches Cloud-Zertifizierungsschema leisten kann und was nicht. Ferner wird analysiert, inwiefern Souveränitätsanforderungen aus (polit-)ökonomischer Sicht sinnvoll bzw. notwendig sind und ob ihre Verankerung in einem Cloud-Zertifizierungsschema juristisch vertretbar erscheint. In Kapitel 4 werden schließlich vor dem Hintergrund des Starts der neuen EU-Kommission mögliche (Aus-)Wege aus der verfahrenen Lage skizziert und Vorschläge für eine künftige resiliente Cloud-Politik präsentiert. Ein Fazit (Kapitel 5) rundet die Untersuchung ab.

Gewährleistung von Privatsphäre und Sicherheit“ [Europäischer Rat (2024), Erklärung von Budapest zum Neuen Deal für die europäische Wettbewerbsfähigkeit, 8. November 2024].

[10] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013.

2 Vorgaben des EU-Rechtsakts zur Cybersicherheit

2.1 Hintergrund

Im April 2019 trat der EU-Rechtsakt zur Cybersicherheit [Cyber Security Act, CSA, (EU) 2019/881[11]] in Kraft. Die Verordnung legt die Ziele, Aufgaben und organisatorischen Aspekte der Agentur der EU für Cybersicherheit (ENISA) fest und schafft zudem einen Rahmen für die Zertifizierung der Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen auf EU-Ebene.

Dieser Zertifizierungsrahmen soll sicherstellen, dass zertifizierte IKT-Produkte, -Dienste und -Prozesse, die in der EU verkauft werden, den EU-Cybersicherheitsstandards entsprechen. Hierzu entwickelt die ENISA sogenannte europäische Schemata für die Cybersicherheitszertifizierung, in denen EU-weit einheitliche Sicherheitsanforderungen und Bewertungskriterien für bestimmte IKT-Produkte, -Dienste und -Prozesse festgelegt werden. Diese Schemata werden dann von der Kommission in Form von Durchführungsrechtsakten beschlossen. Hersteller und Anbieter können dann ihre Produkte, Dienste oder Prozesse nach dem entsprechenden Schema bewerten lassen oder ggf. selbst bewerten. Wenn diese die in dem jeweiligen Schema festgelegten Sicherheitsanforderungen erfüllen, kann für sie ein europäisches Cybersicherheitszertifikat oder eine EU-Konformitätserklärung ausgestellt werden, das bzw. die die Einhaltung der Anforderungen bescheinigt und in allen EU-Mitgliedstaaten anerkannt wird. Europäische Schemata für die Cybersicherheitszertifizierung sollen helfen, die Cybersicherheitsverfahren in der EU zu harmonisieren.[12]

Mit dem EU-Rahmen für die Cybersicherheitszertifizierung sollen insoweit mehrere Ziele verfolgt werden. Er soll

- ein „angemessenes Maß an Cybersicherheit“ sicherstellen,[13]
- eine „Fragmentierung des Binnenmarkts“ bei der Cybersicherheitszertifizierung verhindern,[14]
- das Vertrauen in IKT-Produkte, -Dienste und -Prozesse stärken[15] und
- dazu beitragen, die Entstehung bzw. parallele Existenz kostenträchtiger, vielfältiger, sich widersprechender oder überlappender nationaler Cybersicherheitszertifizierungsschemata zu vermeiden und so die Kosten für Unternehmen zu senken.[16]

2.2 Ausarbeitung europäischer Schemata für die Cybersicherheitszertifizierung

EU-Schemata für die Cybersicherheitszertifizierung werden von der ENISA ausgearbeitet[17] und von der Kommission per Durchführungsrechtsakt beschlossen.[18] In der Regel beauftragt die Kommission[19] die ENISA, ein Schema zu entwickeln, das die Kommission zuvor bereits im sogenannten „fortlaufenden Arbeitsprogramm[20] der Union für die europäische Cybersicherheitszertifizierung“ für bestimmte im

---

11 Verordnung (EU) 2019/881.
12 Erwägungsgrund 95 Verordnung (EU) 2019/881.
13 Art. 1 Abs. 1 lit. b Verordnung (EU) 2019/881.
14 Art. 1 Abs. 1 lit. b Verordnung (EU) 2019/881.
15 Erwägungsgründe 65 und 69 Verordnung (EU) 2019/881.
16 Erwägungsgrund 69 Verordnung (EU) 2019/881.
17 Art. 49 Abs. 1 Verordnung (EU) 2019/881.
18 Art. 49 Abs. 7 Verordnung (EU) 2019/881.
19 Dabei „sollte“ die Kommission auch “die positiven und negativen Auswirkungen ihres Auftrags auf den spezifischen Markt und insbesondere auf KMU, Innovation, die Schranken für den Eintritt in diesen Markt und die Kosten für die Endverbraucher bewerten“ [Erwägungsgrund 84 Verordnung (EU) 2019/881].
20 Art. 47 Verordnung (EU) 2019/881.

Programm aufgelistete[21] IKT-Produkte, -Dienste oder -Prozesse angekündigt hat.[22] Dieses Arbeitsprogramm wird von der EU-Kommission zumindest alle drei Jahre aktualisiert.[23] In begründeten Fällen kann die Kommission – und auch die „Europäische Gruppe für Cybersicherheitszertifizierung (EGCZ)“[24] – die ENISA zudem auffordern, ein Schema auszuarbeiten, das nicht im Arbeitsprogramm enthalten war.[25]

Grundsätzlich gilt, dass alle IKT-Produkte, -Dienste und -Prozesse, die bei der Cybersicherheitszertifizierung einer Bewertung unterzogen werden, den im jeweiligen Schema näher festgelegten Sicherheitsanforderungen genügen müssen. Die Anforderungen sollen „die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten, Funktionen oder Diensten, die von diesen Produkten, Diensten und Prozessen angeboten oder über diese zugänglich gemacht werden, während deren gesamten Lebenszyklus (…) schützen“[26]. Deshalb muss jedes Schema mehrere Sicherheitsziele verwirklichen. Es muss u.a. „gespeicherte, übermittelte oder anderweitig verarbeitete Daten […] gegen eine zufällige oder unbefugte Speicherung, Verarbeitung oder Preisgabe sowie gegen einen zufälligen oder unbefugten Zugriff“ schützen“ und sicherstellen, dass „befugte Personen, Programme oder Maschinen“ […] „nur Zugriff auf die Daten, Dienste oder Funktionen“ [haben], zu denen sie zugangsberechtigt sind“.[27] Darüber hinaus muss bzw. müssen für jedes Schema eine oder mehrere „Vertrauenswürdigkeitsstufen“ – „niedrig“, „mittel“ und/oder „hoch“ – angegeben werden. Die jeweilige Stufe muss in einem „angemessenen Verhältnis“ zu dem Risiko stehen, das mit der Verwendung eines bestimmten IKT-Produkts, -Dienstes oder Prozesses verbunden ist, wobei die Wahrscheinlichkeit und die Auswirkungen eines möglichen Sicherheitsvorfalls zu berücksichtigen sind.[28] Für jede in das Schema aufgenommene Vertrauenswürdigkeitsstufe werden dabei im jeweiligen Schema die entsprechenden – je nach Stufe abweichenden – Sicherheitsanforderungen und Bewertungskriterien festgelegt.[29] Anbieter, die ein Zertifikat für die höchste Vertrauenswürdigkeitsstufe anstreben, müssen dann höheren Anforderungen Genüge leisten bzw. eine strengere Bewertung durchlaufen, als wenn sie ein Zertifikat für eine niedrigere Stufe beantragen wollen.

Jedes von der ENISA entwickelte Schema wird erst anwendbar, nachdem es mittels eines Durchführungsrechtsakts von der Kommission angenommen wurde. Für den Erlass des Rechtsakts kommt das sogenannte „Prüfverfahren“ zur Anwendung.[30] Dieses Verfahren ermöglicht es den Mitgliedstaaten, den Erlass eines neuen Schemas unter bestimmten Voraussetzungen zu verhindern.[31] So muss die Kommission den Entwurf des Durchführungsrechtsakts einem Prüfausschuss unterbreiten, der sich aus Vertretern der Mitgliedstaaten zusammensetzt.[32] Ergänzend sieht die EU-Cybersicherheitsverordnung

[21] Art. 47 Abs. 2 Verordnung (EU) 2019/881.
[22] Art. 48 Abs. 1 Verordnung (EU) 2019/881.
[23] Art. 47 Abs. 5 S. 2 Verordnung (EU) 2019/881.
[24] Die „Europäische Gruppe für die Cybersicherheitszertifizierung“ setzt sich aus Vertretern der nationalen Behörden für die Cybersicherheitszertifizierung oder Vertretern anderer einschlägiger nationaler Behörden zusammen [Art. 62 Verordnung (EU) 2019/881].
[25] Art. 48 Abs. 2 sowie Erwägungsgrund 84 Verordnung (EU) 2019/881.
[26] Art. 46 Abs. 2 Verordnung (EU) 2019/881.
[27] Art. 51 Verordnung (EU) 2019/881.
[28] Art. 52 Abs. 1 Verordnung (EU) 2019/881.
[29] Art. 52 Abs. 3 Verordnung (EU) 2019/881.
[30] Art. 49 Abs. 7 i.V.m. Art. 66 Abs 2 Verordnung (EU) 2019/881, der auf Art. 5 Abs. 4 lit. b der EU-Komitologieverordnung (EU) Nr. 182/2011 verweist (Verordnung (EU) 182/2011 des europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren).
[31] Vgl. Art. 3 Abs. 3 der Verordnung (EU) 182/2011.
[32] Art. 3 Abs. 3 der Verordnung (EU) 182/2011.

vor, dass die Kommission ein europäisches Schema nicht verabschieden darf, bevor der Prüfausschuss eine Stellungnahme abgegeben hat.[33] Lehnt der Ausschuss den Entwurf des Schemas ab, muss die Kommission den Entwurf abändern oder den Berufungsausschuss anrufen.[34] Lehnt auch dieser den Antrag ab, darf die Kommission den Rechtsakt und damit das Schema nicht erlassen.[35]

2.3 Freiwilligkeit oder Pflicht zur Cybersicherheitszertifizierung?

Die Nutzung der europäischen Cybersicherheitszertifizierung ist grundsätzlich „freiwillig". Dies gilt jedoch nur, solange im EU-Recht oder im Recht der Mitgliedstaaten nichts anderes festgelegt ist.[36] Die EU behält sich ausdrücklich vor, eine EU-Zertifizierung für bestimmte IKT-Produkte, -Dienste oder -Prozesse künftig im EU-Recht verbindlich vorzuschreiben.[37] Konkret verleiht etwa die Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)[38] der Kommission unter bestimmten Voraussetzungen die Befugnis, wesentliche[39] und wichtige[40] Einrichtungen per delegiertem Rechtsakt dazu zu verpflichten, nur bestimmte zertifizierte IKT-Produkte und -Dienste zu nutzen oder ein EU-Cybersicherheitszertifikat zu erlangen.[41] Auch die Mitgliedstaaten dürfen wesentliche und wichtige Einrichtungen verpflichten, nur Produkte mit EU-Cybersicherheitszertifikat zu nutzen (siehe dazu auch Box 1).[42] Ferner dürfen sie eine europäische Cybersicherheitszertifizierung insbesondere bei öffentlichen Ausschreibungen und der öffentlichen Auftragsvergaben berücksichtigen.[43]

Box 1: Nutzung von EU-Cybersicherheitszertifizierungsschemata durch wesentliche/wichtige Einrichtungen

Nach der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)[44] „können" die **Mitgliedstaaten** „wesentliche" und „wichtige" Einrichtungen dazu verpflichten, bestimmte IKT-Produkte und -Dienste – dazu können auch Cloud-Dienste zählen – einzusetzen, die[45]

- von der Einrichtung selbst entwickelt oder von Dritten beschafft werden und
- nach einem EU-Cybersicherheitszertifizierungsschema zertifiziert wurden.

Der Entwurf des deutschen „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes" vom Juli 2024 sieht beispielsweise vor, dass das „Bundesministerium des Innern und für Heimat" durch Rechtsverordnung (besonders) wichtigen Einrichtungen vorschreiben können soll, dass diese nur bestimmte, nach einem EU-Cybersicherheitszertifizierungsschema zertifizierte IKT-Produkte und IKT-Dienste verwenden dürfen. Dies gilt dann, wenn[46]

---

33 Art. 66 Abs 2 Verordnung (EU) 2019/881, der auf Art. 5 Abs. 4 lit. b) der Verordnung (EU) Nr. 182/2011 verweist.
34 Art. 5 Abs. 3 Verordnung (EU) Nr. 182/2011.
35 Art. 6 Abs. 3 S. 3 Verordnung (EU) Nr. 182/2011.
36 Art. 56 Abs. 2 Verordnung (EU) 2019/881.
37 Art. 56 Abs. 3 und Erwägungsgrund 92 Verordnung (EU) 2019/881.
38 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 („NIS-2-Richtlinie").
39 Als „wesentliche" Einrichtungen gelten z.B. Unternehmen aus dem Energie-, Verkehrs-, Finanz-, und Gesundheitssektor sowie öffentliche Verwaltungen [Art. 3 NIS-2-Richtlinie].
40 Als „wichtige" Einrichtungen gelten z.B. Unternehmen aus dem Post- und Lebensmittelsektor sowie Unternehmen des verarbeitenden Gewerbes [Art. 3 NIS-2-Richtlinie].
41 Art. 24 Abs. 2 NIS-2-Richtlinie.
42 Art. 24 Abs. 1 NIS-2-Richtlinie.
43 Erwägungsgrund 91 Verordnung (EU) 2019/881.
44 Art. 24 Abs. 1 S. 1 NIS-2-Richtlinie.
45 Art. 24 Abs. 1 NIS-2-Richtlinie.
46 Bundesministerium des Innern und für Heimat (2024), Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz), 22. Juli 2024, siehe §30 Abs. 6 und §56 Abs. 3.

– die Produkte bzw. Dienste für die Erbringung der Dienste der Einrichtung „maßgeblich“ sind, und
– die „Art und das Ausmaß der Risikoexposition der Einrichtung“ einen verpflichtenden Einsatz zertifizierter Produkte bzw. Dienste „erforderlich“ machen.[47]

Ferner kann die **Kommission** für einzelne Kategorien von wesentlichen und wichtigen Einrichtungen festlegen[48], dass diese[49]
– nur bestimmte zertifizierte IKT-Produkte und -Dienste nutzen dürfen oder
– ein EU-Cybersicherheitszertifikat erlangen müssen.

2.4 Unwirksamkeit kollidierender nationaler Schemata für die Cybersicherheitszertifizierung

Ferner sieht der EU-Rechtsakt zur Cybersicherheit (CSA) vor, dass etwaige bestehende nationale Cybersicherheitszertifizierungsschemata unwirksam werden, sofern sie von einem EU-Schema überlagert werden. Dies ist der Fall, wenn bzw. sobald ein geltendes EU-Schema IKT-Produkte, -Dienste und -Prozesse erfasst, die auch Gegenstand eines nationalen Schemas sind. Hierdurch soll eine Zersplitterung des Binnenmarkts vermieden werden.[50] Die Kommission legt den jeweiligen Zeitpunkt, an dem bestehende nationale Schemata unwirksam werden, in ihrem Beschluss fest, mit dem sie das EU-Schema annimmt. Erfasste IKT-Produkte dürfen dann nicht mehr national zertifiziert werden; bereits ausgestellte nationale Zertifikate bleiben jedoch bis zum Ende ihrer Geltungsdauer gültig.[51] Die Mitgliedstaaten dürfen dann grundsätzlich auch keine neuen Schemata einführen, die mit einem EU-Schema kollidieren. Dagegen bleiben nationale Schemata für IKT-Produkte, Dienste und -Prozesse bestehen, die nicht unter ein solches EU-Schema fallen.[52] Die Mitgliedstaaten dürfen kollidierende nationale Schemata aber ausnahmsweise dann einführen oder beibehalten, sofern sie dies aus „Gründen der nationalen Cybersicherheit“ für erforderlich erachten.[53]

2.5 Weitere Grundsätze für EU-Cybersicherheitszertifizierungsschemata

Schließlich gelten für Cybersicherheitszertifizierungsschemata insbesondere die beiden folgenden weiteren Grundsätze: Erstens „sollten“ die EU- Cybersicherheitszertifizierungsschemata „nichtdiskriminierend“ sein[54]; zweitens „sollten“ sie „in einheitlicher Weise in allen Mitgliedstaaten eingeführt werden“. Die EU-weit einheitliche Einführung soll „Zertifizierungsshopping“ – d.h. die gezielte Beantragung der Zertifizierung in dem Mitgliedstaat mit dem geringstem Anforderungsniveau – verhindern.[55]

---

47 Hat die Kommission bereits delegierte Rechtsakte zum verpflichtenden Einsatz solcher Schemata vorgeschrieben, haben diese Rechtsakte Vorrang gegenüber einer via Rechtsverordnung erlassenen Regelung. Das Bundesministerium des Innern und für Heimat muss sich ferner vor dem Erlass einer Rechtsverordnung mit anderen Ressorts abstimmen. Auch muss es prüfen, ob überhaupt ein Schemata vorhanden ist und ob ausreichend zertifizierte IKT-Produkte bzw. IKT-Dienste am Markt verfügbar sind.

48 Eine solche Festlegung erfolgt über den Erlass delegierter Rechtsakte. Ein solcher Erlass ist nur möglich, sofern ein „unzureichendes Niveau der Cybersicherheit“ festgestellt wurde [Art. 24 Abs. 2 NIS-2-Richtlinie].

49 Art. 24 Abs. 2 NIS-2-Richtlinie.

50 Erwägungsgrund 94 Verordnung (EU) 2019/881.

51 Art. 57 Abs. 3 Verordnung (EU) 2019/881.

52 Art. 57 Abs. 1 S. 2 Verordnung (EU) 2019/881.

53 Erwägungsgrund 94 Verordnung (EU) 2019/881.

54 Erwägungsgrund 69 Verordnung (EU) 2019/881.

55 Erwägungsgrund 70 Verordnung (EU) 2019/881.

3 Das EU-Schema zur Zertifizierung der Cybersicherheit von Cloud-Diensten (EUCS)

3.1 Grundsätzliches

Am 9. Dezember 2019 hat die Kommission die ENISA mit der Ausarbeitung eines EU-Cybersicherheitszertifizierungsschemas für Cloud-Dienste [„European Cybersecurity Certification Scheme for Cloud Services (EUCS)"] beauftragt.[56] Der Auftrag wurde von der Kommission insbesondere damit begründet, die Cybersicherheitsstandards für Cloud-Dienste im EU-Binnenmarkt stärken und straffen zu wollen. Derzeit gibt es in der EU einen Flickenteppich an Cybersicherheitsstandards für Cloud-Dienste. In Deutschland legt etwa der sogenannte C5-Kriterienkatalog (Cloud Computing Compliance Criteria Catalogue) des Bundesamts für Sicherheit in der Informationstechnik (BSI) Mindestanforderungen an sicheres Cloud-Computing fest.[57] Die Kommission betrachtet die unterschiedlichen nationalen Schemata in den EU-Mitgliedstaaten als „Herausforderung für die Zertifizierung von Cloud-Diensten" und das EUCS als Mittel zur Überwindung dieser Problematik.[58] Das EUCS soll die Cybersicherheitszertifizierung von Cloud-Diensten in der EU im Einklang mit internationalen Standards und bewährten Branchenpraktiken harmonisieren und einen Übergang von den derzeitigen nationalen Zertifizierungssystemen hin zu einem einheitlichen, EU-weit gültigen Cybersicherheitszertifizierungssystem für Cloud-Dienste schaffen. Zugleich hält die Kommission ein EUCS für notwendig, um „die Nutzung von Cloud-Diensten in Europa zu fördern", da Cloud-Dienste eine grundlegende Technologie für die Entwicklung in vielen technologischen Bereichen darstellen.[59]

Im Dezember 2020 legte die ENISA einen ersten Entwurf des EUCS vor und stellte ihn zur Konsultation.[60] Der EUCS-Entwurf sieht die Etablierung eines „horizontalen" Schemas für eine breite Palette an Cloud-Diensten – Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), etc. – vor.[61] Das EUCS legt grundlegende Sicherheitsanforderungen für Cloud-Dienste fest, die sich an bestehenden nationalen Systemen und internationalen Normen orientieren. Es ist als freiwilliges Schema konzipiert, deckt drei Vertrauenswürdigkeitsstufen – niedrig, mittel und hoch – ab und soll eine Zertifizierung für drei Jahre gewähren, die erneuert werden kann.[62] Das EUCS soll als „technisches Instrument" fungieren, welches den potenziellen Kunden von Cloud-Diensten Informationen zur Verfügung stellt und es ihnen so ermöglichen soll, fundierte Entscheidungen zu treffen.[63] Es soll die Cybersicherheit in der gesamten Cloud-Lieferkette gewährleisten und eine Grundlage für darauf aufbauende sektorale Schemata bilden.[64]

Seit die ENISA ihren ersten Entwurf für das EUCS vorgelegt hat, hat sie ihn bereits mehrfach überarbeitet. Dennoch hat die Kommission das EUCS bis heute – und damit auch nach knapp vier Jahren – nicht final per Durchführungsrechtsakt angenommen. Dies ist insbesondere auf eine seit Langem geführte

---

56 EU-Kommission (2019), Towards a more secure and trusted cloud in Europe, siehe hier.

57 Bundesamt für Sicherheit in der Informationstechnik, Kriterienkatalog C5, siehe hier. Cloud-Dienste können sich auf Basis der strengen Kriterien dieses Prüfstandards von Wirtschaftsprüfern nach „BSI C5" zertifizieren lassen und erhalten dann nach erfolgreicher Prüfung ein sogenanntes C5-Testat, vgl. FAQ C5 des BSI.

58 EU-Kommission (2021), EU Cloud Certification Scheme, 9. Juni 2021, siehe hier.

59 ENISA (2020a), EUCS – Cloud Services Scheme, December 2020, S. 10, siehe hier.

60 ENISA (2020b), Cloud Certification Scheme: Building Trusted Cloud Services Across Europe, ENISA launches a public consultation on a new draft candidate cybersecurity certification scheme in a move to enhance trust in cloud services across Europe, Press Release, December 22, 2020, siehe hier.

61 ENISA (2020a), S. 11.

62 ENISA (2020b).

63 ENISA (2020a), S. 11.

64 ENISA (2020b); ebenso ENISA (2021), Consultation on the draft EUCS, siehe hier.

Diskussion über die mögliche Aufnahme von sogenannten „Souveränitätsanforderungen“ in das Schema zurückzuführen. Auf diese Diskussion soll im Folgenden genauer eingegangen werden.

3.2 Diskussion über Souveränitätsanforderungen in einem künftigen EUCS

Unter „Souveränitätsanforderungen“ versteht man Anforderungen, die die Souveränität der EU sicherstellen oder steigern sollen. Gemeint sind insbesondere Anforderungen, die verhindern sollen, dass Drittstaaten auf bestimmte Informationen zugreifen, wie etwa die Pflicht, Daten nur in der EU zu speichern oder Verträge ausschließlich dem EU-Recht zu unterwerfen. Die Debatte um die Einführung von Souveränitätsanforderungen wird nachfolgend anhand einer Reihe ausgewählter unterschiedlicher Fassungen des EUCS veranschaulicht.

Erste Fassung des EUCS-Entwurfs von Dezember 2020: Im ersten Entwurf eines EUCS im Dezember 2020 durch die ENISA spielten Souveränitätsanforderungen allenfalls eine untergeordnete Rolle. Die ENISA betonte vielmehr ausdrücklich, dass das geplante EUCS-Schema keine Anforderungen festlegen sollte, die den geografischen Standort für die Speicherung oder Verarbeitung der Daten beschränken oder das anwendbare Recht einschränken. Jedoch verlangte sie, dass Cloud-Dienste-Anbieter über den geografischen Standort der Daten und das anwendbare Recht Transparenz wahren müssten. So sollten Cloud-Dienste-Anbieter u.a. Informationen über die Standorte aller Systemkomponenten bereitstellen müssen, auf denen Daten ihrer Kunden gespeichert oder verarbeitet werden. Der erste Entwurf des EUCS sah für die Zertifizierung insgesamt drei Vertrauenswürdigkeitsstufen vor – niedrig (basic), erheblich (substantial) und hoch (high). Eine Zertifizierung für die Vertrauenswürdigkeitsstufe „hoch“ sollte für alle Cloud-Dienste geeignet sein, die spezielle – über die mittlere Stufe hinausgehende – Sicherheitsanforderungen für „unternehmenskritische Daten und Systeme“ erfüllen sollen und in der Lage sind, „das Risiko von dem neuesten Stand der Technik entsprechenden Cyberangriffen durch Akteure mit umfangreichen Fähigkeiten und Ressourcen möglichst gering zu halten.[65] In dieser höchsten Sicherheitsstufe sollten Cloud-Dienste zusätzlich dokumentieren müssen, von welchen Standorten welche Supportleistungen erbracht werden. Diese Informationen sollten dann nach erfolgter Zertifizierung gemeinsam mit dem Zertifikat veröffentlicht werden.[66]

Fassung des EUCS-Entwurfs vom Mai 2023: Es blieb jedoch nicht bei dieser Herangehensweise. In einem überarbeiteten Entwurf schlug die ENISA im Mai 2023 erstmals spezifische, über reine Transparenzvorgaben hinausgehende Souveränitätsanforderungen vor[67]. So führte die ENISA u.a. eine Reihe neuer Anforderungen ein, die die Unabhängigkeit des bewerteten Cloud-Dienstes von Nicht-EU-Rechtsvorschriften sicherstellen sollten und insbesondere Anforderungen in Bezug auf den Standort der Datenspeicherung und -verarbeitung, den Standort von Zugriffsberechtigten sowie die wirksame Kontrolle des Cloud-Dienste-Anbieters umfassten.[68] Zugleich schlug die ENISA vor, die Vertrauenswürdigkeitsstufe „hoch“ in zwei separate, sogenannte „Evaluierungsstufen“ (Evaluation levels, EL) – CS-EL3 und CS-EL4 – aufzuteilen. Während die Evaluierungsstufe CS-ELS3 wie die Vertrauenswürdigkeitsstufe „Hoch“ im ursprünglichen Entwurf für alle Cloud-Dienste geeignet sein sollte, die spezielle – über die zweite, mittlere Stufe hinausgehende – Sicherheitsanforderungen für unternehmenskritische Daten und Systeme erfüllen sollen, zielt die Evaluierungsstufe CS-ELS4 auf die „sensibelsten“ Cloud-Dienste ab. Darunter sollen alle Cloud-Dienste zu verstehen sein, die besonders sensible

65 ENISA (2020a), S. 20; vgl. auch Art. 52 Abs. 7 Verordnung (EU) 2019/881.
66 ENISA (2020a), S. 11 und 151 (DOC-=3 Data Processing and Storage) und 215 (F 6.2).
67 ENISA (2023), EUCS – Cloud Services Scheme, V.1.0.319, May 2023.
68 ENISA (2023), S. 6.

personenbezogene oder nicht-personenbezogene Daten verarbeiten, deren Kompromittierung „voraussichtlich zu einer Verletzung der öffentlichen Ordnung, der öffentlichen Sicherheit, des Lebens oder der Gesundheit von Menschen oder des Schutzes des geistigen Eigentums“ führen würde.[69]

Die Souveränitätsanforderungen wurden in einem neuen Anhang J näher definiert. Sie teilten sich in vier Gruppen ein. Die Anforderungen der ersten Gruppe (PUA-01) sollte den Vorrang des EU-Rechts sicherstellen. Die Anforderungen der zweiten Gruppe (PUA-02) enthielten Vorgaben zu den Standorten, an denen zertifizierte Cloud-Dienste betrieben und gewartet und Kundendaten gespeichert und verarbeitet werden. Die Anforderungen der dritten Gruppe (PUA-03) sollten dazu dienen, Zugriffe durch Mitarbeiter und Geschäftspartner außerhalb der EU zu kontrollieren. Durch die Anforderungen der vierten Gruppe (PUA-04) sollte schließlich sichergestellt werden, dass Drittstaaten keinerlei Kontrolle über die zertifizierten Cloud-Dienste-Anbieter erlangen bzw. ausüben können.

Einige dieser neuen Anforderungen der ersten Gruppe sollten für alle Vertrauenswürdigkeitsstufen gelten. So sollten Cloud-Dienste-Anbieter bereits für eine Zertifizierung nach der unteren und mittleren Vertrauenswürdigkeitsstufe (nun als Evaluierungsstufen CS-EL1 und CS-EL2 bezeichnet) sicherstellen müssen, dass ihre Verträge über Cloud-Dienstleistungen dem Recht eines EU-Mitgliedsstaats unterliegen, nur nach diesem Recht auszulegen sind und ausschließlich Gerichte bzw. Spruchkörper in den EU-Mitgliedstaaten für die Beilegung von Vertragsstreitigkeiten für zuständig erklären. Die strengsten Souveränitätsanforderungen sollten jedoch für die Vertrauenswürdigkeitsstufe „hoch“ gelten. Der EUCS-Entwurf von 2023 sah daher für die Evaluierungsstufen CS-EL3 und CS-EL4 u.a. die nachfolgend aufgeführten zusätzlichen Anforderungen vor. Dabei gingen die restriktiven Anforderungen für die CS-EL4-Stufe noch deutlich über die CS-EL3-Stufe hinaus:[70]

1. Vorrang des EU-Rechts und Unabhängigkeit vom Nicht-EU-Recht:

Die Cloud-Dienste-Anbieter sollten

- zur Sicherstellung der Unabhängigkeit vom Nicht-EU-Recht ab der Evaluierungsstufe CS-EL3 zusätzlich verpflichtet sein, bestimmte Risiken für den Fall der möglichen extraterritorialen Anwendung von kollidierendem Nicht-EU-Recht in ihre globale Risikobewertung einbeziehen; dazu gehört insbesondere das Risiko, dass ausländische Behörden über dieses Drittstaatsrecht Zugang zu wirtschaftlich sensiblen geschäftlichen Informationen und Geschäftsgeheimnissen erhalten, für deren Verarbeitung keine vorherige Einwilligung des Eigentümers der Informationen oder der in ihnen genannten juristischen Personen vorlag (Anforderung PUA-01.2H),
- ihren Kunden auf Anforderung Informationen über Restrisiken für deren eigene Risikobewertung zur Verfügung stellen müssen (Anforderung PUA-01.3H),
- sich vertraglich verpflichten, nur Ermittlungsanfragen zu berücksichtigen, die auf der Grundlage von EU- oder mitgliedstaatlichem Recht gestellt werden (Anforderung PUA-01.5H), und

[69] ENISA (2023), S. 26, 28, 31 und 32. Zu diesen besonders sensiblen Daten gehören laut der ENISA erstens gesetzlich geschützte Geheimnisse wie Daten über Regierungsberatungen, die nationale Sicherheit und Verteidigung, die Außenpolitik oder Gerichtsverfahren. Zweitens soll die Evaluierungsstufe CS-EL 4 auch „für den Schutz der Privatsphäre“, das Arztgeheimnis sowie für Geschäftsgeheimnisse gelten, einschließlich Informationen über Produktionsmethoden, Wirtschaft und Finanzen, Geschäfts- oder Industriestrategien. Drittens erfasse die Stufe CS-EL 4 alle Daten, die für die Erfüllung wesentlicher staatlicher Aufgaben wie die Wahrung der nationalen Sicherheit, die Aufrechterhaltung der öffentlichen Ordnung und den Schutz des Lebens und der Gesundheit von Menschen erforderlich sind. Dagegen ist die Evaluierungsstufe CS-EL3 „für Anwendungsfälle gedacht, in denen die Unabhängigkeit von Nicht-EU-Recht ein wichtiger Faktor ist“, allerdings in einem Ausmaß, das je nach dem genauen Anwendungsfall und der Rechtsstruktur des Cloud-Anbieters von Anbieter zu Anbieter variieren kann (S. 28).

[70] ENISA (2023), S. 301–306.

- über diese bloße vertragliche Verpflichtung hinaus technische und organisatorische Maßnahmen ergreifen, um sicherzustellen, dass sie etwaigen Ermittlungsanfragen, die nicht auf Grundlage des EU-Rechts oder des Rechts eines EU-Mitgliedstaats gestellt wurden, tatsächlich nicht nachkommen; diese letztgenannte Anforderung war jedoch nur auf der höchsten Evaluierungsstufe CS-EL 4 zu erfüllen (Anforderung: PUA-01.6H).

2. Betrieb des Cloud-Dienstes in der EU:

- Für eine Zertifizierung nach der Evaluierungsstufe CS-EL3 sollten Cloud-Dienste-Anbieter zwar nicht verpflichtet sein, ihre Dienste einschließlich Support generell nur von Standorten in der EU aus zu erbringen, zu verwalten und alle Kundendaten ausschließlich an Standorten in der EU zu speichern und zu verarbeiten. Sie sollten aber Transparenz über diese Standorte wahren und ihren Kunden vertraglich mindestens eine Option anbieten müssen, bei der alle angegebenen Standorte in der EU liegen (Anforderung PUA 02.1H i.V.m. DOC-02.1H).[71]
- Für eine Zertifizierung nach der Evaluierungsstufe CS-EL4 beschränkten sich die Anforderungen demgegenüber nicht lediglich auf eine vertragliche Kundenoption zur Datenspeicherung und -verarbeitung in der EU, sondern verpflichteten den Cloud-Dienste-Anbieter generell zur vollständigen Datenlokalisierung und -verarbeitung innerhalb der EU. So sollten alle Systemkomponenten, an denen der Cloud-Dienste-Anbieter oder seine Unterdienstanbieter Kundendaten speichern und verarbeiten, ausschließlich in der EU situiert sein. Darüber hinaus sollten Cloud-Dienste nur von Standorten innerhalb der EU aus verwaltet und überwacht und auch Supportleistungen grundsätzlich nur von solchen Standorten aus erbracht werden dürfen. Allenfalls einzelne, genau aufgelisteten Support-Aktivitäten und unter außergewöhnlichen im Vertrag geregelten Umständen auch bestimmte andere Aktivitäten sollten ausnahmsweise aus einem Drittstaat erbracht werden dürfen. Auch hier sollte der Anbieter aber auch eine Option anbieten müssen, die eine vollständige Datenlokalisierung in der EU ohne die genannten Ausnahmen gewährleistet (Anforderung PUA-02.1H).

3. Kontrolle von Zugriffen, die durch Mitarbeiter und Geschäftspartner in Drittstaaten erfolgen

Die Cloud-Dienste-Anbieter sollten

- ab der Evaluierungsstufe CS-EL3 zudem sicherstellen, dass lediglich solche Mitarbeiter Zugriff auf Daten des Cloud-Kunden erhalten, die sich entweder in der EU befinden oder bei dem Zugriff von einem vorab geprüften und in der EU ansässigen Mitarbeiter überwacht werden (Anforderung: PUA-03.1H), und darüber hinaus
- verpflichtet werden, alle Dienstleister, die Support für funktionale Komponenten des Cloud-Dienstes erbringen, vorab zu überprüfen oder durch einen in der EU befindlichen geprüften Mitarbeiter überwachen zu lassen, der notfalls in Echtzeit eingreifen und weitere Zugriffe verbieten kann (Anforderung PUA-03.2H). Alle Wartungshandlungen sollten protokolliert, überprüft und archiviert werden (Anforderung PUA-03.3H).

4. EU-Hauptsitz und Anforderungen an die Unternehmenskontrolle des Cloud-Dienste-Anbieters

- Die sensibelsten und daher nach der Evaluierungsstufe CS-EL4 zu zertifizierenden Cloud-Dienste sollten schließlich zusätzliche – über die Stufe CS-EL3 hinausgehende – Anforderungen erfüllen

[71] ENISA (2023), S. 306.

müssen, um eine „effektive Kontrolle über den Cloud-Dienste-Anbieter“[72] sicherzustellen. So sah der Entwurf vor, dass sich sowohl der eingetragene Hauptsitz als auch die globale Hauptverwaltung dieser Anbieter in der EU befinden müssten (Anforderung PUA-04.1H). Ferner wollte die ENISA vorschreiben, dass Unternehmen aus Drittstaaten keine effektive Kontrolle[73] über den Cloud-Dienste-Anbieter ausüben dürfen – und zwar weder direkt noch indirekt und weder allein noch gemeinsam mit anderen Unternehmen (Anforderung PUA-04.2H). Hierdurch sollte das Risiko gemindert werden, dass „einflussreiche Mächte außerhalb der EU die Vorschriften, Normen und Werte der EU untergraben“.[74]

Die wichtigsten zusätzlichen Souveränitätsanforderungen des EUCS-Entwurfs vom Mai 2023 lassen sich daher wie folgt zusammenfassen:

- Die Verträge über die Erbringung zertifizierter Cloud-Dienste müssen dem Recht eines Mitgliedstaats unterliegen und festlegen, dass für Streitigkeiten im Zusammenhang mit den Verträgen nur Gerichte oder Spruchkörper in der EU zuständig sind.
- Um eine Zertifizierung der Evaluierungsstufe CS-EL3 zu erhalten, darf der Cloud-Dienste-Anbieter auf Daten seiner Kunden nur unter der Kontrolle von Mitarbeitern zugreifen, die sich einer speziellen Überprüfung unterzogen haben und in der EU ansässig sind. Zudem muss er eine Risikobewertung im Zusammenhang mit der extraterritorialen Anwendung von Nicht-EU-Gesetzen vornehmen. Dagegen beschränkte der Entwurf den geografischen Standort der Daten oder ihrer Verarbeitung auf dieser Stufe nicht grundsätzlich auf die EU, sondern verlangte vom Anbieter lediglich Transparenz über seine Standorte und die Gerichtsbarkeit.[75]
- Um eine Zertifizierung der strengsten Evaluierungsstufe CS-EL4 zu erhalten, muss der Anbieter dagegen zusätzlich seinen Hauptsitz in der EU haben müssen und darf keiner wirksamen Kontrolle durch Nicht-EU-Unternehmen unterliegen. Zudem müssen alle Standorte, an denen Kundendaten gespeichert oder sonst verarbeitet werden oder von denen aus Support erbracht oder der Cloud-Dienst verwaltet oder gewartet wird, innerhalb der EU liegen. Obgleich das EUCS als „technisches Instrument“ konstruiert wurde, schlug die ENISA für die Evaluierungsstufe CS-EL4 folglich im Vergleich zur ersten Entwurfsfassung Beschränkungen des anwendbaren Rechts, des geografischen Standorts der Verarbeitung der Daten und des Unternehmenssitzes des Cloud-Dienste-Anbieters vor.[76]

Fassung des EUCS-Entwurfs vom März 2024: Nach langen Diskussionen und Interventionen auch der Regierungen einzelner Mitgliedstaaten finden sich derartige Souveränitätsanforderungen in der jüngsten Fassung des EUCS aus dem März 2024 nicht mehr.[77] Neben der unteren und mittleren Stufe gibt es zwar weiterhin die Vertrauenswürdigkeitsstufe „hoch“; innerhalb dieser wird jedoch nicht länger zwischen den Evaluierungsstufen CS-EL3 und CS-EL4 unterschieden. Die Stufe „hoch“ soll wie bisher für alle Cloud-Dienste in Betracht kommen, die dafür konzipiert wurden, „unternehmenskritische Daten und Systeme“ zu schützen – wie etwa sensible und vertrauliche Daten von Unternehmen und Regierungen. Diese Vertrauenswürdigkeitsstufe sei auch für Cloud-Dienste geeignet, die entwickelt

72 ENISA (2023), S. 25 und 26.
73 Hinsichtlich des Begriffs „Kontrolle“ verwies die ENISA auf die EG-Fusionskontrollverordnung (EG) Nr. 139/2004.
74 ENISA (2023), S. 305.
75 ENISA (2023), S. 15.
76 ENISA (2023), S. 15.
77 ENISA (2024), EUCS – Cloud Services Scheme, V1.0.413, March 2024.

wurden, um sektorspezifischen Anforderungen im Hinblick auf weltweite Geschäftstätigkeiten zu genügen. Hier denkt die ENISA explizit an den Finanzsektor.[78]

Die oben dargestellten restriktiven Souveränitätsvorgaben sollen dagegen explizit entfallen, Anhang J wurde aus dem Entwurf wieder entfernt. Allein die „Anforderungen an den Vorrang des EU-Rechts" bei der Gestaltung von Verträgen sollen bestehen bleiben (Anforderung: A.5, CO-05.1B), wonach Cloud-Dienste-Anbieter „in erster Linie" innerhalb des EU-Rechts und des Rechts der Mitgliedstaaten operieren müssen. Wie im EUCS-Entwurf von 2023[79] müssen die Verträge zwischen Cloud-Dienste-Anbietern, die eine Zertifizierung ihres Cloud-Dienstes anstreben, und Nutzern ihres Cloud-Dienstes auf jeder der drei Vertrauenswürdigkeitsstufen dem Recht eines EU-Mitgliedsstaats unterliegen, nur nach diesem Recht auszulegen sein und ausschließlich Gerichte bzw. Spruchkörper in den EU-Mitgliedstaaten für die Beilegung von Vertragsstreitigkeiten für zuständig erklären, nicht aber Gerichte, Tribunale oder Schiedsstellen aus Drittstaaten.[80]

Wie bereits in der Ursprungsfassung müssen Cloud-Dienste-Anbieter unabhängig von der Vertrauenswürdigkeitsstufe schließlich Transparenz über die Gerichtszuständigkeit und alle Standorte wahren, an denen Daten verarbeitet, gespeichert und gesichert werden.[81]

Damit ist die Einfügung strikter Souveränitätskriterien in das EUCS jedoch noch nicht vom Tisch. Vielmehr wurde seither hinter den Kulissen über eine Wiedereinfügung solcher Kriterien in den Entwurf diskutiert, wenn diese auch zuletzt als unwahrscheinlich bezeichnet wurde.[82] Einen finalen Entwurf hat die ENISA nach wie vor nicht veröffentlicht.

3.3 Was kann ein EU-Cybersicherheitszertifizierungsschema für Cloud-Dienste leisten und was nicht?

Die Etablierung eines EU-Cybersicherheitszertifizierungsschemas für Cloud-Dienste ist grundsätzlich sinnvoll. Denn ein solches Schema kann bestehenden Informationsasymmetrien begegnen. Häufig können die Nutzer von Cloud-Diensten – ob Verbraucher, Unternehmen oder staatliche Institutionen – nur bedingt einschätzen, wie es um die Cybersicherheit der von ihnen (noch nicht) nachgefragten Cloud-Dienste bestellt ist. Dieses Informationsdefizit schmälert ihre Zahlungsbereitschaft für die vermeintlich sicheren Cloud-Dienste. In der Folge haben die Cloud-Dienste-Anbieter auch weniger Anreize, in die Cybersicherheit ihrer Dienste zu investieren. Die Märkte für Cloud-Dienste weisen folglich regelmäßig Charakteristika von „Zitronenmärkten" (Markets for lemons) auf.

Das geplante EUCS kann einen wichtigen Beitrag dazu leisten, dieser Problematik zu begegnen. Bei entsprechender Ausgestaltung kann es sowohl den Markt für cybersichere Cloud-Dienste beleben als auch das Vertrauen potenzieller Nutzer in die Dienste stärken. Das EUCS kann somit ein Vehikel dafür sein, das Vertrauen in die Nutzung von Cloud-Diensten per se und die damit einhergehende Überlassung von Daten an „vertrauenswürdige" Dritte zu stärken. So zeigt eine jüngst veröffentlichte Umfrage, dass bei der Auswahl von Cloud-Anbietern das Vertrauen in die IT-Sicherheit, Datenschutz und Compliance die wichtigste Rolle (99%) spielt. Auch sind Befürchtungen hinsichtlich des unberechtigten

78 ENISA (2024), S. 24.
79 ENISA (2023), Anhang J, Anforderung PUA-01.1B.
80 ENISA (2024), S. 100.
81 ENISA (2024), S. 145.
82 Gkritsi, E. (2024), Sovereignty requirements for cloud providers unlikely to make it to Commission's proposal for implementing act, 26. Juni 2024, s. hier.

Zugriffs auf sensible Daten für 64% und des Verlustes von Daten für 52% der Befragten relevante Hürden für die Umsetzung von Cloud-Projekten.[83] Die Stärkung des Nutzervertrauens kann jedoch nur dann erreicht werden, wenn das Schema bei den Nutzern als glaub- und vertrauenswürdig erachtet wird. Zudem muss Folgendes immer bedacht werden: Die Zertifizierung der Cybersicherheit von Cloud-Diensten geht tendenziell mit einer Verteuerung der Dienste einher. Dies kann die Entwicklung eines florierenden Marktes für cybersichere Cloud-Dienste ausbremsen. Und obwohl ein EUCS ein wichtiges Element der europäischen Cybersicherheitspolitik darstellt, ist es kein Allheilmittel. Denn es adressiert insbesondere zwei Problematiken nicht: Erstens verbleiben auch weiterhin Anreize bei Cloud-Dienst-Nutzern, Cyberrisiken bei der Auswahl eines solchen Dienstes nicht in volkswirtschaftlich nötigem Umfang Bedeutung zu schenken. Denn auch ein EUCS verhindert nicht, dass die Nutzer regelmäßig nicht die vollen Kosten eines Cybersicherheitsvorfalls tragen müssen, denn sie können Schäden an andere Akteure auslagern. Diese negativen Folgen eines Vorfalls preisen sie nicht in ihr Entscheidungskalkül mit ein („Nichtinternalisierung externer Effekte“). Zweitens kann ein EUCS Trittbrettfahrerverhalten nicht verhindern. Denn oft profitieren Dritte zwar davon, dass ein Bürger, ein Unternehmen oder der Staat einen cybersicheren Cloud-Dienst nutzt, leisten für diesen „Zusatzgewinn“ jedoch keinen eigenen Beitrag an den zahlenden Bürger, das Unternehmen oder den Staat. Die Käufer bzw. Nutzer des cybersicheren Cloud-Dienstes werden für die Generierung eines derartigen positiven externen Effekts nicht honoriert. Dies schmälert jedoch wiederum ihre Bereitschaft, in cybersichere Dienste zu investieren, da sie darauf vertrauen, dass Dritte die mit sichereren Cloud-Diensten verbundenen Mehrkosten schon tragen werden. Für die Adressierung dieser beiden Problematiken – Nichtinternalisierung externer Effekte und Trittbrettfahrerverhalten – bedarf es anderer spezifischer Politikmaßnahmen. Einer dieser Maßnahmen war beispielsweise die Verabschiedung des EU-Cyberresilienzgesetzes (Cyber Resilience Act, s. cep**Analyse**)[84].

Es ist sachgerecht, dass das EUCS vordergründig als freiwilliges Zertifizierungsschema konzipiert ist. Denn wäre der Erwerb eines Zertifikats für die Anbieter von Cloud-Diensten in jedem Fall verpflichtend, könnte dies als unnötige und teure Markteintrittsbarriere wirken und Innovationen ausbremsen. Eine Pflicht zur Cybersicherheitszertifizierung erscheint grundsätzlich erstens nur in hochsensiblen Anwendungsbereichen vertretbar – welche dies sind, ist in erster Linie eine (gesellschafts-)politische Entscheidung.[85] Zweitens scheint sie in den Fällen vertretbar, in denen die Nutzung eines „unsicheren“ Cloud-Dienstes durch einen privaten, kommerziellen oder staatlichen Anwender größere Cybersicherheitsrisiken für Dritte hervorruft oder hervorrufen könnte.

3.4 Sind Souveränitätsanforderungen geeignet?

3.4.1 Zweck und potenzielle Vorteile der Anforderungen

Die zwischenzeitlich avisierte Implementierung von Souveränitätsanforderungen in einem künftigen EUCS hat insbesondere drei Dimensionen: eine industriepolitische, eine sicherheits- bzw. geopolitische

[83] Bitkom (2024), Cloud Report 2024, Welche Rolle spielt die Cloud für die deutsche Wirtschaft?, 3. Juli 2024.

[84] Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung, s. cep**Analyse**).

[85] Eine solche Entscheidung wurde im Wesentlichen im Rahmen der Festlegung von wesentlichen und wichtigen Einrichtungen im Rahmen der Überarbeitung der Richtlinie über Maßnahmen zur Gewährleistung eines hohes gemeinsames Sicherheitsniveaus von Netz und Informationssystemen in der EU (sogenannte NIS-2-Richtlinie (EU) 2016/1148) gefällt (s. neue Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der EU).

und eine den gemeinsamen Binnenmarkt in den Blick nehmende Dimension. Diese drei Dimensionen müssen sowohl getrennt als auch zusammen gedacht werden.

Im industriepolitischen Kontext sollen Souveränitätsanforderungen einerseits die Markteintrittshürden für Anbieter von Cloud-Diensten aus Drittstaaten erhöhen bzw. ihre weitere Teilnahme am Markt erschweren und die Abhängigkeit von diesen Anbietern verringern. In diesem Sinne dienen die Souveränitätsanforderungen somit als ein Instrument der Marktabschottung. Auf der anderen Seite sollen sie als Maßnahme fungieren, um Cloud-Dienste-Anbietern aus der EU den Markteintritt zu erleichtern bzw. ihren bereits vorhandenen Fußabdruck im Markt aufrechtzuerhalten oder sogar auszubauen. In diesem Sinne dienen die Anforderungen mithin als Instrument zur Marktöffnung.[86] Bereits in ihrer Mitteilung zur „Gestaltung der digitalen Zukunft Europas“ im Februar 2019 hob die Kommission die Bedeutung der Gewährleistung der „Integrität und Widerstandsfähigkeit“ der Dateninfrastrukturen, -netze und -kommunikation in der EU hervor und forderte, dass in der EU die „richtigen Bedingungen“ etabliert werden müssten, damit Europa „eigene Schlüsselkapazitäten entwickeln und einsetzen“ und „seine Abhängigkeit von anderen Teilen der Welt bei den wichtigsten Technologien verringern kann“. Dies sei für die „digitale Souveränität“[87] Europas entscheidend.[88] Auch betonte die Kommission in ihrem Auftrag an die ENISA zur Ausarbeitung des EUCS, dass dieses nicht allein ein Instrument der Stärkung der Cybersicherheit von Cloud-Diensten im Binnenmarkt darstellen solle, sondern auch eines zur „Förderung des Einsatzes von Cloud-Diensten in Europa".[89] Souveränitätsanforderungen sind damit auch ein Mittel, um die Wettbewerbsfähigkeit der EU im Technologiebereich zu stärken[90] und um sicherzustellen, dass EU-Unternehmen dort, wo technologische Souveränität für erforderlich gehalten wird, „weiterhin Fuß fassen“ können und Europa somit „nicht auf die Entwicklung seines heimischen Technologiesektors verzichten“ kann[91]. Zudem können EU-weit einheitliche Souveränitätsanforderungen Größenvorteile ermöglichen, da Anbieter von Cloud-Diensten sich nicht nach unterschiedlichen nationalen Vorgaben zertifizieren lassen müssen. Dies kann auch die Kosten für Nutzer der zertifizierten Cloud-Dienste potenziell senken. Außerdem ließen sich Souveränitätsanforderungen auch mit dem Argument rechtfertigen, dass sie bestehende Monopolisierungs- bzw. Oligopolisierungstendenzen auf den EU-Märkten für Cloud-Dienste abschwächen und so die Resilienz stärken können[92] – decken doch

[86] Auch Blancato, F. G. (2024) sieht die Bemühungen zur Wahrung der Datenhoheit – als Teilaspekt digitaler Souveränität – als „integralen Bestandteil eines industriepolitischen Instrumentariums“, mit dem die EU lokale Cloud-Anbieter vor ausländischer Konkurrenz schützen will [Blancato, F. G. (2024), The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem, Policy & Internet, 16(1), 12-32].

[87] Kreutzer et al. (2022) definieren „digitale Souveränität“ als „die Fähigkeit, eigene Ziele selbstbestimmt umsetzen zu können, ohne aufgrund unzureichender bzw. fehlender Kontrolle über digitale Schlüsseltechnologien und -kompetenzen im selbstbestimmten Handeln eingeschränkt oder gar behindert zu werden. Das Konzept der digitalen Souveränität ist sowohl von Autarkie als auch von Fremdbestimmung abzugrenzen, da Souveränität oftmals nur in der Vernetzung mit anderen Akteuren erlangt werden kann“ [Kreutzer, S. et al. (2022), Wie Europa seine digitale Souveränität wiederherstellen kann].

[88] EU-Kommission (2020b), Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Gestaltung der digitalen Zukunft Europas, COM(2020) 67, 19. Februar 2020.

[89] ENISA (2020a), S. 10.

[90] Kenneth Propp, Peter Swire and Josh Fox (2023), Oceans Apart: The EU and US Cybersecurity Certification Standards for Cloud Services, 11. Juli 2023.

[91] EU-Kommission (2024a).

[92] Vgl. dazu auch A. Wolf (2024), cepInput No. 14, Resilience Auctions for Net-Zero Technologies, An Effective Market-based Measure to Shield the Green Transition?, 24 September 2024, S. 6. Folgt man dieser Argumentation wären Souveränitätsanforderungen obsolet, sobald die Monopol- bzw. Oligopolstellungen überwunden wären [A. Wolf (2024), S. 6].

die drei US-Unternehmen Amazon, Microsoft und Google momentan über 60% des EU-Cloud-Marktes ab.[93]

Gleichzeitig haben Souveränitätsanforderungen ein sicherheitspolitisches und geopolitisches Momentum, welches sich ebenfalls in dem Terminus der „digitalen Souveränität" spiegelt. So besteht ein großes öffentliches Interesse daran, europäischen Unternehmen und Behörden „Zugang zu sicheren […] Cloud-Infrastrukturen und -Diensten" ermöglichen und diesen Zugang auch aufrechterhalten zu können.[94] Es geht letztlich beim Aufbau von „minimum viable clouds" – also „vertrauenswürdigen EU-Cloud-Umgebungen mit ausreichenden und sicheren Fähigkeiten" – um eine Frage der Wahrung der nationalen Sicherheit.[95] Dies gilt insbesondere für Informationen von hoher nationaler Tragweite, bei denen die Wahrung der Datensicherheit in der Cloud für die Mitgliedstaaten von immenser Bedeutung ist und strategische Priorität hat.[96] So sollen Souveränitätsanforderungen denn auch eine gewisse „Immunität gegenüber Nicht-EU-Recht"[97] sicherstellen. Auch sollen sie die Informationssicherheit stärken und dazu beitragen, die Hoheit über Daten – insbesondere über als besonders sensibel erachtete Daten und Informationen – zu wahren. Entsprechend betont die ENISA die Notwendigkeit, Daten, deren Kompromittierung potenzielle negative Auswirkungen auf die öffentliche Ordnung, die öffentliche Sicherheit, das menschliche Leben, die Gesundheit oder den Schutz des geistigen Eigentums haben kann, in besonderem Maße zu schützen.[98] Zudem können Souveränitätsanforderungen auch als eine Art Vorkehrung gegen eine gezielte Verweigerung des Zugangs zu genutzten Cloud-Diensten aus Drittstaaten oder auch gegen den ungeplanten Ausfall oder Wegfall dieser Dienste betrachtet werden[99], gerade auch vor dem Hintergrund wachsender geopolitischer Unsicherheiten und Risiken. Kommen Cloud-Dienste als kritische digitale Technologie aus nur einem oder wenigen Ländern und besteht diesbezüglich eine „hohe Konzentration des weltweiten Angebots", bedeutet dies auch eine hohe Abhängigkeit von der Industrie- und Handelspolitik dieser Länder, die diese „geostrategische Machtposition" […] dann als „diplomatisches Druckmittel" nutzen könnten.[100,101] Ferner sollen Souveränitätsanforderungen unterstreichen, dass die EU auch künftig in der Lage sein will, eigens geschaffene Regelungen implementieren und durchsetzen („Regelungssouveränität") und sich etwaigen Anfragen etwa von Sicherheits- und Strafverfolgungsbehörden aus Drittstaaten entziehen zu können.[102]

Einen dritten Zweck, den einheitliche EU-weite Souveränitätsanforderungen zu erfüllen versprechen, ist die Vermeidung einer Zersplitterung solcher Vorgaben im Binnenmarkt. Frankreich dient hier als Paradebeispiel. So etablierte die französische Regierung eine „Cloud im Zentrum"-Doktrin, die

93 Synergy Research Group (2024).

94 Siehe hier.

95 Alexandre Gomes and Maaike Okano-Heijmans (2024), Too late to act? Europe's quest for cloud sovereignty, Clingendael, Netherlands Institute of International Relations, März 2024. Die Autoren betonen, dass die Diversifizierung der europäischen Lösungen kein Luxus sei, sondern eine Notwendigkeit.

96 Raman, S. (2023), Two Visions of Digital Sovereignty. Joint PIJIP/TLS Research Paper Series, American University Washington College of Law.

97 „Immunität gegenüber Nicht-EU-Recht" meint letztlich, dass Cloud-Anbieter, die Daten von Cloud-Nutzern in der EU verarbeiten oder speichern, allein EU-Recht unterworfen sein sollten. Das Recht eines Drittstaats sollte für ihn keine Geltung haben.

98 ENISA (2023).

99 Raman, S. (2023).

100 A. Wolf (2024), S. 6.

101 Das solche oder ähnlich gelagerte Schritte nicht ganz unrealistisch sind, zeigt die Ankündigung des designierten US-Vizepräsidenten JD Vance, wonach die USA die Unterstützung der Nato verweigern könnten, sollte die Plattform „X" in der EU übermäßig reguliert werden (s. auch hier).

102 Kenneth Propp (2022), European Cybersecurity Regulation Takes a Sovereign Turn, European Law Blog, 12. September 2022.

öffentlichen Einrichtungen in Frankreich bei der Verwendung von Cloud-Diensten Souveränitätsvorgaben macht.[103] Das Land führte zusätzlich ein verpflichtendes Cybersicherheitszertifizierungsschema unter dem Titel „SecNumCloud“ ein. Zertifizierungen nach dem Schema werden von der nationalen Agentur für Cybersicherheit (ANSSI) vergeben. Das Schema enthält ebenfalls Vorgaben zum Schutz vor Nicht-EU-Recht.[104,105] Es gilt gemeinhin als Blaupause für die im Rahmen des EUCS zwischenzeitlich vorgesehenen Souveränitätsanforderungen.[106] Würden weitere Mitgliedstaaten diesem Beispiel folgen, wären unterschiedlichste Regelungen in der EU die Folge bzw. diese würden sich verstetigen. Damit würde jedoch zum einen potenziellen Wettbewerbsverzerrungen Vorschub geleistet. Dies gilt insbesondere für Unternehmen, die in unterschiedlichen Mitgliedstaaten ansässig sind, aber miteinander konkurrieren. Gälten für diese Unternehmen unterschiedlich strenge Voraussetzungen bei der Auswahl erlaubter Cloud-Dienste, würde dies zu Wettbewerbsvorteilen bzw. zu Wettbewerbsnachteilen für die betroffenen Unternehmen führen. Zudem müssten Unternehmen in den einzelnen Mitgliedstaaten gegebenenfalls unterschiedliche und konträre Anforderungen erfüllen, was insbesondere für Cloud-Dienste-Anbieter, die in mehreren Mitgliedstaaten aktiv sind, höhere Kosten und Mehraufwand zur Folge hätte. Durch harmonisierte Souveränitätsvorgaben im EUCS ließen sich nicht nur solche Wettbewerbsverzerrungen vermeiden, sondern einheitliche Anforderungen schüfen zugleich Erleichterungen bei der Rechtsanwendung und Rechtskonsistenz.

3.4.2 Befürchtungen und potenzielle Risiken der Souveränitätsanforderungen

Das zentrale Ziel eines jeden EU-Rahmens für die Cybersicherheitszertifizierung ist es, ein „angemessenes Maß an Cybersicherheit“ sicherzustellen.[107] Dies gilt somit auch für das geplante EUCS. Insbesondere muss es auf der höchsten Vertrauenswürdigkeitsstufe darauf ausgerichtet sein, „das Risiko von dem neuesten Stand der Technik entsprechenden Cyberangriffen durch Akteure mit umfangreichen Fähigkeiten und Ressourcen möglichst gering zu halten“.[108] Es wird nun teilweise betont, dass Souveränitätsanforderungen die Cybersicherheit nicht etwa erhöhen, sondern eher beeinträchtigen könnten[109]. So würde für Cloud-Nutzer etwa der Zugang zu möglicherweise ausgereifteren und cybersichereren (Nicht-EU) Cloud-Lösungen bzw. -Diensten beschränkt. Durch Lokalisierungsvorgaben wären zudem mehr Daten- bzw. Rechenzentren nötig, welche kompromittiert werden könnten. Es bräuchte einen Zuwachs an (qualifiziertem) Personal zur Unterhaltung der verschiedenen Cloud-Dienste-Standorte, welches ggf. nicht immer in ausreichendem Maße zur Verfügung steht. Mehr Standorte und Mitarbeiter erhöhen zudem die potenzielle Angriffsfläche für Angreifer. Auch der Zugang zu und Austausch über (mögliche) Cyberbedrohungen wäre erschwert, wenn diesbezügliche Informationen nicht grenzüberschreitend geteilt werden können. Zudem könnten Souveränitätsanforderungen zu einer verringerten Verteilung von (sensiblen) Informationen führen und mithin der Entstehung von Konzentrationsrisiken Vorschub leisten. Insgesamt würden sie außerdem zu einer

[103] Die Doktrin wurde im Juli 2021 beschlossen und Ende Mai 2023 aktualisiert (s. hier).
[104] SecNumCloud sieht etwa vor, dass der Cloud-Dienste-Anbieter seinen Sitz in einem EU-Mitgliedstaat haben muss und sieht Einschränkungen bei den Eigentumsverhältnissen vor.
[105] Premier ministre (2022), Agence nationale de la sécurité des systèmes d’information, Prestataires de services d’informatique en nuage (SecNumCloud), référentiel d’exigences, Version 3.2, 8. März 2022.
[106] Christakis, T. (2024), The “Zero Risk” Fallacy: International Data Transfers, Foreign Governments’ Access to Data and the Need for a Risk-Based Approach.
[107] Art. 1 Verordnung (EU) 2019/881.
[108] ENISA (2023), EUCS – Cloud Services Scheme, V.1.0.319, May 2023, S. 25.
[109] Blancato, F. G. (2024) weist darauf hin, dass Bemühungen der Politik zur Territorialität von Daten letztlich dem Konzept von Daten an sich widersprechen. Werden Daten in der Cloud verarbeitet oder gespeichert, geschieht dies in der Regel nicht an einem spezifischen Ort und in einer bestimmten Jurisdiktion.

Verkomplizierung des Managements von Cyberrisiken beitragen.[110,111,112] Und nicht zuletzt könnte die mit Souveränitätsanforderungen einhergehende Marktabschottung dazu führen, dass Cloud-Nutzer auf einen oder wenige konforme Anbieter zurückgreifen müssten und so in eine (neue) Abhängigkeit getrieben werden, was aus einer Sicherheitsperspektive keine sinnvolle Strategie darstellen würde.[113]

Neben der Gefahr einer Schwächung der Cybersicherheit durch Souveränitätsanforderungen bestehen auch noch weitere Befürchtungen. So könnten sie als protektionistischer Schritt aufgefasst werden und Drittstaaten ihrerseits dazu verleiten, Gegen- bzw. Vergeltungsmaßnahmen einzuführen, welche EU-Cloud Anbietern den Zugang zu den Märkten der Drittstaaten erschweren oder versperren. Dies wäre insbesondere für global tätige Anbieter schädlich, die in diesen Märkten aktiv sind bzw. dort präsent sein wollen. Der internationale Handel würde gestört. Auf der anderen Seite begrenzen Souveränitätsanforderungen das Marktangebot, schränken die Wahlfreiheit für Cloud-Dienste-Nachfrager ein und schwächen damit den Wettbewerb. Dies erhöht möglicherweise die Preise für die Nutzer der Dienste und somit ihre Kosten. Auch abseits von den Fähigkeiten der Drittstaats-Cloud-Anbieter hinsichtlich der Abwehr von Cyberbedrohungen und Bekämpfung von Cybersicherheitsvorfällen, die man durch Souveränitätsanforderungen zu verlieren droht, bedeuten diese Anforderungen auch einen potenziellen Verlust des Zugangs zu – für die eigene Wettbewerbspositionierung entscheidenden – Innovationen und Features dieser Cloud-Dienst-Anbieter. Und nicht zuletzt könnten Datenlokalisierungsvorgaben auch zu (nachhaltigkeitsbezogenen) Ineffizienzen beitragen, da die Standortwahl von Daten- und Rechenzentren beschränkt wird. Diese könnten gegebenenfalls nicht länger dort positioniert werden, wo die Energie am grünsten, die Energiekosten am geringsten und die Verfügbarkeit der Ressource Wasser am größten ist.[114]

Zuletzt weist Christakis, T. (2024) darauf hin, dass Cloud-Anbieter, die die Souveränitätsvorgaben zu erfüllen – und somit Immunität gegenüber Nicht-EU-Recht – versprechen, dieses Versprechen in Bezug auf die USA wohl gar nicht in jedem Fall abgeben könnten, sofern sie selbst auch in den USA tätig sind. Denn sie könnten dann dennoch von US-Recht betroffen sein und wären gegebenenfalls genötigt, Anfragen von US-Behörden nachzugehen.[115] Nach dieser Einschätzung wären die Anforderungen an die Souveränität teilweise unwirksam und damit letzten Endes unnötig.

3.4.3 Sind Souveränitätsanforderungen im Interesse (potenzieller) Cloud-Nutzer?

Inwiefern Souveränitätsanforderungen auf Nutzerseite angesichts dieser Gemengelage auf Zustimmung stoßen würden, ist nicht eindeutig festzustellen. Zwar zeigt die bereits oben zitierte Umfrage, dass das Vertrauen in die IT-Sicherheit, Datenschutz und Compliance für potenzielle Cloud-Nutzer eine zentrale Rolle spielt. Ob jedoch Rechenzentren beispielsweise in Deutschland oder in der EU situiert sein und/oder aus einem vertrauenswürdigen Herkunftsland stammen sollten, ist nur für knapp 60% der Befragten von hoher Bedeutung. Gleichzeitig sagen jedoch 53% bzw. 96% der Umfrageteilnehmer, dass für sie die USA bzw. China nicht als Standort einzelner Rechenzentren in Frage kommt, und für 98% ist der Standort der Rechenzentren per se ein relevanter Faktor. Und eine große Anzahl der

[110] Raman, S. (2023).
[111] Swire, P., & Kennedy-Mayo, D. (2022), The Effects of Data Localization on Cybersecurity. Georgia Tech Scheller College of Business Research Paper, 4030905.
[112] Bauer, M., & Lamprecht, P. (2023), The economic impacts of the proposed EUCS exclusionary requirements estimates for EU member states (No. 04/2023), ECIPE Occasional Paper.
[113] Alexandre Gomes and Maaike Okano-Heijmans (2024).
[114] Raman, S. (2023); Bauer, M., & Lamprecht, P. (2023); Alexandre Gomes and Maaike Okano-Heijmans (2024).
[115] Christakis, T. (2024).

Umfrageteilnehmer messen auch der Leistungsfähigkeit der angebotenen Cloud-Dienste eine gewichtige Rolle bei (97%).[116] Ob strikte Souveränitätsanforderungen daher in der Praxis tatsächlich gewollt sind, erscheint derzeit offen.

3.5 Juristische Perspektive – Rechtmäßigkeit von Souveränitätsanforderungen

3.5.1 Vereinbarkeit mit dem EU-Rechtsakt zur Cybersicherheit (CSA)

Zunächst stellt sich die Frage, ob bzw. inwieweit die Festlegung von Souveränitätsanforderungen in einem EUCS durch die EU-Kommission von dem EU-Rechtsakt zur Cybersicherheit (CSA) als „Basisrechtsakt" gedeckt ist. Wäre dies nicht der Fall würde die Kommission sich bei einer Verabschiedung eines EUCS mit Souveränitätsanforderungen u.U. außerhalb ihres vom CSA vorgesehenen Kompetenzrahmens bewegen.

Aber welchen Rahmen gibt der CSA vor? Art. 1 Abs. 2 des CSA stellt zunächst klar, dass die Kompetenzen der Mitgliedstaaten für Tätigkeiten in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das staatliche Handeln im strafrechtlichen Bereich unberührt bleiben. Dadurch werden die genannten Bereiche aber nicht generell vom Geltungsbereich des CSA ausgenommen. Ausgenommen von der EU-Kompetenz ist jedoch der enge Bereich der nationalen Sicherheit der Mitgliedstaaten, der nach Art. 4 Abs. 2 S. 3 des EU-Vertrags (EUV) in der alleinigen Zuständigkeit der EU-Mitgliedstaaten verbleibt.[117] Weil die EU in diesem Bereich keine Regelungen treffen darf und durfte, kann der CSA von vornherein keine rechtmäßige Grundlage für Souveränitätsanforderungen in einem EUCS bilden, die in den Bereich der den Mitgliedstaaten vorbehaltenen nationalen Sicherheit fallen. Solche Regelungen in einem EUCS wären damit nicht rechtmäßig.

Souveränitätsanforderungen dürften aber in den meisten Fällen nicht den engen Bereich der nationalen Sicherheit betreffen. Der europäische Zertifizierungsrahmen für die Cybersicherheit wurde geschaffen, um „die Cybersicherheit in der EU zu erhöhen.[118] „Cybersicherheit" bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.[119] Eine „Cyberbedrohung" wiederum ist jeder Umstand, jedes Ereignis oder jede Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.[120] Weil der CSA nicht alle „Anforderungen an die Cybersicherheit" sämtlicher IKT-Produkte, -Dienste und -Prozesse im Einzelnen festlegen kann, sollen die europäischen Schemata für die Cybersicherheitszertifizierung ergänzend gewährleisten, dass die nach ihren Vorgaben zertifizierten IKT-Produkte, -Dienste und -Prozesse bestimmten Anforderungen genügen, deren Ziel es ist, die in Art. 51 des CSA geregelten Sicherheitsziele zu verwirklichen.[121] Zu diesen Sicherheitszielen gehört es vor allem, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste, die von diesen Produkten, Diensten und Prozessen angeboten oder über diese zugänglich gemacht werden, während ihres gesamten Lebenszyklus zu schützen.[122] Die Schemata müssen die relevanten Cybersicherheitsziele regeln und im Einzelnen die

[116] Bitkom (2024), Cloud Report 2024, Welche Rolle spielt die Cloud für die deutsche Wirtschaft?, 3. Juli 2024.
[117] Näher zur nationalen Sicherheit siehe noch unten Kapitel 3.5.2.
[118] Art. 46 Abs. 1 Verordnung (EU) 2019/881.
[119] Art. 2 Nr. 1 Verordnung (EU) 2019/881.
[120] Art. 2 Nr. 8 Verordnung (EU) 2019/881.
[121] Vgl. Erwägungsgrund 75 der Verordnung (EU) 2019/881.
[122] Vgl. Erwägungsgrund 75 sowie Art. 51 der Verordnung (EU) 2019/881 und insbesondere dessen lit a), b) und c).

Modalitäten festlegen, wie diese Ziele für bestimmte IKT-Dienste (hier Cloud-Dienste) erreicht werden sollen.

Fraglich ist, inwieweit es sich bei den im EUCS-Entwurf enthaltenen Souveränitätsanforderungen – insbesondere bei dem Sitzerfordernis, dem Erfordernis der Datenlokalisierung und den Anforderungen an die Unternehmenskontrolle – um Anforderungen an die „Cybersicherheit" handelt. Dagegen könnte etwa vorgebracht werden, dass diese Anforderungen nicht rein technischer, sondern eher rechtlicher Natur sind. Die Anforderungen sollen aber zumindest auch den vorgenannten Sicherheitszielen dienen, denn ihr Zweck besteht darin, unbefugte Zugriffe aus Drittstaaten auf Daten und Cloud-Dienste zu verhindern. Welche Anforderungen die ENISA bzw. die Kommission in einem Cybersicherheitszertifizierungsschema für Cloud-Dienste im Detail regeln darf und welche nicht, schreibt der CSA nicht ausdrücklich vor; insbesondere legt er nicht fest, dass die Schemata ausschließlich technische Details regeln dürfen. Seinem Art. 52 Abs. 3 lässt sich entnehmen, dass im Schema die „Sicherheitsanforderungen" – dies umfasst die „Sicherheitsfunktionen" der Dienste sowie die Kriterien für die Strenge und Gründlichkeit der Bewertung – zu regeln sind. Was eine „Sicherheitsfunktion" ist, definiert der CSA nicht. Ob Anforderungen an die Unabhängigkeit vom Drittstaatsrecht eine „Sicherheitsfunktion" eines Cloud-Dienstes darstellen, ist dennoch fraglich. Zudem verweist der CSA an mehreren Stellen darauf, dass in den Schemata auf „technische Spezifikationen" und/oder Normen verwiesen werden kann bzw. muss. So verlangt er, dass die europäischen Schemata für die Cybersicherheitszertifizierung auf dem auf internationaler und nationaler Ebene bereits Vorhandenen und erforderlichenfalls auf den von Gremien und Konsortien erstellten technischen Spezifikationen aufbauen „sollten", wobei die derzeitigen Stärken genutzt und Schwachstellen bewertet und behoben werden sollten.[123] Entsprechend schreibt er vor, dass jedes Schema als Mindestelement unter anderem eine Bezugnahme auf die für die Bewertung maßgeblichen technischen Normen und Spezifikationen enthalten muss.[124] Dies spricht dafür, dass die Kommission in den Schemata zumindest in erster Linie technische Aspekte regeln darf und soll.

Zu beachten ist ferner, dass die Kommission ein von der ENISA ausgearbeitetes Schema wie das EUCS in einem sogenannten Ausschussverfahren als Durchführungsrechtsakt erlässt.[125] Zwar durfte und darf der EU-Gesetzgeber der Kommission im CSA die Befugnis übertragen, wichtige Details der Zertifizierung in Durchführungsverordnungen zu regeln.[126] Der Gesetzgeber ist aber nach der Rechtsprechung des Europäischen Gerichtshofs (EuGH) verpflichtet, alle wesentlichen Aspekte selbst zu regeln.[127] Die wesentlichen Bestimmungen einer Materie sind in der Grundregelung zu regeln. Der Kommission zur Durchführung übertragen werden darf daher nicht der Erlass von Bestimmungen, welche politische Entscheidungen erfordern, die in die eigene Zuständigkeit des EU-Gesetzgebers fallen.[128] Als „wesentlich" erachtet der EuGH lediglich Vorschriften, durch die die grundsätzliche Ausrichtung der EU-Politik umgesetzt wird.[129] Zwar enthält Art. 291 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der Durchführungsrechtsakte regelt, anders als Art. 290, der die Befugnis der EU-Kommission

[123] EG 71 Verordnung (EU) 2019/881. Ähnlich sieht EG 69 vor, dass die Schemata nichtdiskriminierend sein und sich auf europäische oder internationale Normen stützen sollten, sofern diese Normen nicht unwirksam oder unangemessen im Hinblick auf die Erreichung der legitimen Ziele der Union in diesem Bereich sind.

[124] Art. 54 Abs. 1 lit. c) Verordnung (EU) 2019/881.

[125] Art. 49 Abs. 7, Art. 66 Abs. 2 Verordnung (EU) 2019/881.

[126] Eckhardt. P. / Hoffmann, A., Cybersicherheit Teil 2 – Zertifizierung, cep**Analyse** Nr. 16/2028.

[127] Der Wesentlichkeitsvorbehalt spiegelt sich auch im Gesetzesvorbehalt des EU-Rechts bei der Einschränkung von Grundrechten wider, der in Art. 52 Abs. 1 der EU-Grundrechtecharta kodifiziert wurde. Näher dazu siehe unten Kapitel 3.5.5.

[128] EuGH, Urteil vom 5. September 2012, Rs. C-355/10 – EP ./. Rat, ECLI:EU:C:2012:516, Rn. 64, 65.

[129] EuGH, Urteil vom 27. Oktober 1992, Rs. C-240/90, Deutschland./.Kommission, ECLI:EU:C:1992:408, Rn. 37.

zum Erlass sogenannter delegierte Rechtsakte regelt, keinen expliziten Verweis darauf, dass die wesentlichen Festlegungen dem Gesetzgeber vorbehalten sind. Dies ist aber auch nicht notwendig, da Vollzugsakte naturgemäß die wesentlichen Elemente des Basisrechtsakts nicht beeinflussen können.[130]

Die Grenzen der Befugnisse der Kommission sind anhand der Hauptziele des Basisrechtsakts – hier des CSA – zu beurteilen. Die Kommission darf alle zur Durchführung erforderlichen und zweckmäßigen Maßnahmen ergreifen, soweit diese nicht gegen die Grundregelung im Basisrechtsakt verstoßen, deren wesentliche Grundzüge nicht antasten und ihren Anwendungsbereich nicht verändern.[131] Denn durch Durchführungsverordnungen soll lediglich eine nähere Konkretisierung der Regeln im Basisrechtsakt zur Wahrung dessen einheitlicher Durchführung in den Mitgliedstaaten erfolgen.[132]

Zwar wollen die Befürworter der Souveränitätsanforderungen diese Anforderungen für die gesamte EU einheitlich regeln, und der CSA gibt mit den Sicherheitszielen, Elementen und Wirkungen der Schemata auch die grundsätzliche Ausrichtung der Zertifizierung selbst vor. Durch die Aufnahme restriktiver Souveränitätskriterien, die den Cloud-Dienste-Anbietern vorschreiben, alle Daten in der EU zu lokalisieren, ihren Hauptsitz in der EU zu haben und immun gegen Drittstaatsrecht zu sein, würde die Kommission aber nicht lediglich vorhandene technische oder rechtliche Kriterien zur Stärkung der Cybersicherheit in der EU im Wege einer unpolitischen Ausfüllung „konkretisieren“. Vielmehr würde sie wesentliche Aspekte ergänzen und dem EUCS hierdurch eine neue Dimension hinzufügen, was in Durchführungsrechtsakten rechtlich nicht möglich ist.

Welche Aspekte als wesentlich einzustufen sind, ist objektiv zu beurteilen. Dabei sind die Merkmale und Besonderheiten des betreffenden Sachgebiets zu berücksichtigen.[133] Auch im Bereich der delegierten Rechtsakte wird eine Entscheidung umso eher als „wesentlich“ erachtet, je politischer sie ist.[134] Zumindest zwingende Souveränitätsanforderungen wie das Erfordernis des verpflichtenden Unternehmenssitzes und der Unternehmenskontrolle sowie der Datenlokalisierung in der EU weisen eine grundlegende politische Bedeutung auf, da sie den Cloud-Markt in der EU wesentlich beeinflussen können und zudem handelspolitische und andere Risiken bergen.[135] Durch sie würden möglicherweise europäische Cloud-Dienste-Anbieter gestärkt; zugleich könnte es für Anbieter aus Drittstaaten schwerer werden, auf dem europäischen Markt tätig zu werden, vor allem, wenn es um Cloud-Dienste auf der höchsten Vertrauenswürdigkeitsstufe geht. Gegner der Souveränitätsanforderungen behaupten zudem, dass EU-Behörden und Unternehmen dadurch gezwungen sein könnten, auf Anbieter mit wirtschaftlich unzureichenden, unsichereren oder schlicht teureren Leistungen auszuweichen.[136] Angesichts der möglichen vielschichtigen politischen Auswirkungen muss zumindest die Entscheidung über die Einführung verpflichtender Souveränitätsanforderungen als „wesentlich“ angesehen werden.

Welchen Weg die EU insoweit wählt, um sich vor Einflussnahme aus Drittstaaten zu schützen, ist daher eine Frage der grundsätzlichen und damit dem EU-Gesetzgeber vorbehaltenen Ausrichtung der EU-Politik. Dies bestätigt nicht zuletzt die langjährige kontroverse und ergebnislose politische Diskussion unter den Mitgliedstaaten über die Einfügung von Souveränitätskriterien in den EUCS-Entwurf. Im Rahmen der Debatte haben Staaten wie die Niederlande daher zu Recht die Auffassung vertreten, dass

[130] Schmidt, F., in: von der Groeben,H./Schwarze, J./Hatje, A., AEUV, 7. Aufl. 2015, Art. 291 Rn. 14.
[131] Gellermann, M., in: Streinz, R., EUV/AEUV, 3. Aufl. 2018, Rn. 12.
[132] Nettesheim, M., in: Grabitz, E./Hilf, M./Nettesheim, M., AEUV Art. 291 Rn. 40.
[133] EuGH, Urteil vom 5. September 2012, Rs. C-355/10 – EP ./. Rat, ECLI:EU:C:2012:516, Rn. 67f.
[134] Nettesheim, M., (a.a.O.), Art. 291 Rn. 41.
[135] Näher dazu bereits oben Kapitel 3.4.2.
[136] Propp (2023), Oceans apart: The EU and US Cybersecurity Certification Standards for Cloud Services, abrufbar hier.

das Thema der Souveränitätsanforderungen auf der europäischen politischen Ebene behandelt werden muss.[137] Im Ergebnis handelt es sich bei der verpflichtenden Einführung der dargestellten Souveränitätsanforderungen um eine wesentliche politische Entscheidung, die nicht durch die Kommission und die ENISA, sondern nur durch den Gesetzgeber getroffen werden kann.[138] Die EU sollte daher etwaige Souveränitätsanforderungen gesetzlich regeln. Ein ordentliches EU-Gesetzgebungsverfahren würde zum einen eine in transparenterer Weise geführte Debatte über die Sinnhaftigkeit und die Auswirkungen der Souveränitätsanforderungen unter Beteiligung des Europäischen Parlaments ermöglichen. Zum anderen bedarf es solider Folgenabschätzungen und Untersuchungen der Marktakzeptanz, um eine fundierte Entscheidung darüber zu treffen, ob – und wenn ja welche – Souveränitätsanforderungen eingeführt werden sollen.

3.5.2 Kompetenzen zur Regelung von Souveränitätsanforderungen, Subsidiarität und Verhältnismäßigkeit gegenüber den Mitgliedstaaten

Bei der gesetzlichen (Neu-)Regelung EU-weiter Souveränitäts- und Cybersicherheitsanforderungen könnte die EU sich möglicherweise auf die Kompetenz zur Harmonisierung des Binnenmarkts [Art. 114 AEUV] stützen. Wie das Beispiel der französischen SecNumCloud zeigt, hat die französische Regierung bereits ein verpflichtendes Cybersicherheitszertifizierungsschema eingeführt, das ebenfalls Souveränitätsanforderungen enthält. Eine einheitliche Regelung auf EU-Ebene würde eine Fragmentierung des Binnenmarkts durch unterschiedliche Souveränitätsanforderungen in den Mitgliedstaaten verhindern und so dazu beitragen, einen funktionierenden Binnenmarkt für Cloud-Dienstleistungen zu schaffen. Um ausschließlich spezifische Anforderungen an Cloud-Dienste zu regeln, müsste die EU aber ggf. vorrangig die grundfreiheitsspezifische Kompetenznorm zur Harmonisierung des Dienstleistungsverkehrs in Art. 53 Abs. 1 i.V.m. Art. 62 AEUV nutzen. Auf Basis dieser Norm könnte die EU allerdings lediglich eine Richtlinie erlassen, um die Vorschriften der Mitgliedstaaten über die „Aufnahme und Ausübung“ von Cloud-Dienstleistungen in der EU zu koordinieren. Die EU sollte dies genau prüfen und die Wahl ihrer Rechtsgrundlage hinreichend begründen.

Die Kompetenzen der EU enden jedoch, sobald die Regelungen den Schutz der nationalen Sicherheit der Mitgliedstaaten berühren. Wie bereits dargelegt, fällt der Schutz der nationalen Sicherheit nach Art. 4 Abs. 2 S. 3 des Vertrags über die Europäische Union (EUV) weiterhin in die alleinige Verantwortung und Zuständigkeit der EU-Mitgliedstaaten.[139] Die EU darf folglich in Bereichen, die in die nationale Sicherheit der Mitgliedstaaten fallen, keine Souveränitätsanforderungen regeln bzw. muss diese Bereiche in ihren Regelungen ausklammern. Wie der EuGH im Schrems II-Urteil entschieden hat, betrifft die genannte Regelung im EUV ausschließlich „die Mitgliedstaaten“ [140] und damit die innereuropäische Kompetenzverteilung – sie schützt die EU-Mitgliedstaaten vor zu weitgehenden Eingriffen der EU in diese wichtige nationale Kernkompetenz. Dritte (z.B. Drittstaaten oder Unternehmen aus Drittstaaten) können sich dagegen nicht auf diese Bestimmung berufen.[141]

---

[137] Stellungnahme der Niederlande zum Non-paper von DE, ES, FR und IT zu den EUCS-Anforderungen an die Immunität gegenüber Nicht-EU-Gesetzen (2021), abrufbar hier.

[138] So allgemein (d.h. nicht auf den vorliegenden Fall bezogen) Ruffert, M., in Calliess, C./Ruffert, M., EUV/AEUV, 6. Aufl. 2022, AEUV Art. 290 Rn. 15.

[139] Es handelt sich somit um einen mitgliedstaatlichen Zuständigkeitsvorbehalt, vgl. Obwexer, W., in: Von der Groeben, H./Schwarze, J./Hatje, A., Europäisches Unionsrecht, 7. Auflage 2015, Art. 4 EUV Rn. 46.

[140] EuGH, Schrems II (Fn. **Fehler! Textmarke nicht definiert.**), Rn. 81.

[141] EuGH, Schrems II (Fn. **Fehler! Textmarke nicht definiert.**), Rn. 81.

Der Begriff der „nationalen Sicherheit“ ist enger auszulegen als der Begriff der „öffentlichen Sicherheit. Er umfasst nur solche Störungen der öffentlichen Sicherheit, die nationale Bedeutung haben, also die die Sicherheit des Staates selbst betreffen.[142] Welche Souveränitätsanforderungen für welche Anbieter, Daten und Systeme in den engen Bereich der nationalen Sicherheit fallen, gilt es noch genauer zu prüfen.

Souveränitätsanforderungen gehen aber in der Regel über den Schutz der nationalen Sicherheit hinaus und können auch weiter gesteckten legitimen Zielen dienen. Diese können von der Schaffung einer Vertrauensgrundlage für die umfassendere Nutzung von Cloud-Diensten mittels einer durch sie ausgelösten Stärkung der Cybersicherheit über einen verbesserten Schutz von Daten bis hin zum Schutz der öffentlichen Sicherheit und Ordnung in den EU-Mitgliedstaaten reichen. Bei der Rechtssetzungskompetenz für den Binnenmarkt handelt es sich um eine zwischen der EU und den Mitgliedstaaten geteilte Kompetenz.[143] Sowohl die EU als auch die Mitgliedstaaten dürfen zur Verwirklichung des Binnenmarkts grundsätzlich Souveränitätsanforderungen regeln. Es handelt sich jedoch um eine konkurrierende Kompetenz dergestalt, dass die Mitgliedstaaten ihre Handlungsbefugnis verlieren, sofern und soweit die Union ihre Zuständigkeit ausgeübt hat.[144]

Solange und insoweit die EU noch nicht tätig geworden ist und ein EUCS erlassen bzw. Souveränitätsanforderungen für Cloud-Dienste geregelt hat, dürfen die Mitgliedstaaten ihrerseits auf nationaler Ebene noch eigene Schemata für die Cybersicherheitszertifizierung aufrechterhalten. Sobald die Union ihre eingeräumte Rechtsetzungskompetenz jedoch genutzt hat, tritt für die nationalen Gesetzgeber in den Mitgliedstaaten eine Sperrwirkung ein.[145] Diese ergibt sich sowohl aus Art. 2 Abs. 2 S. 2 und 3 AEUV als auch konkret aus Art. 57 Abs. 1-3 CSA. Nach dieser Regelung im CSA dürfen die Mitgliedstaaten – sobald die EU ein EUCS erlassen hat – grundsätzlich keine konkurrierenden Schemata für die Cybersicherheitszertifizierung mehr einführen oder aufrechterhalten; bestehende Schemata werden unwirksam.

Macht die EU von ihrer Kompetenz Gebrauch und regelt Souveränitätsanforderungen bzw. ein EU-weit gültiges EUCS, muss sie – neben der Kompetenzausübungsschranke in Bezug auf die nationale Sicherheit – das Subsidiaritätsprinzip gemäß Art. 5 Abs 3 und das Verhältnismäßigkeitsprinzip nach Art. 5 Abs. 4 des Vertrags über die Europäische Union (EUV) beachten. Zwar kann ein EU-weit hohes (technisches) Cybersicherheitsniveau grundsätzlich am besten auf EU-Ebene erreicht werden. Jede EU-weite Regelung von Cybersicherheits- und Souveränitätsanforderungen für Cloud-Dienste greift jedoch in die Befugnis der Mitgliedstaaten ein, das Cybersicherheitsniveau oder andere Sicherheitsinteressen in ihrem Staat eigenständig und selbstbestimmt zu regeln. Eine verpflichtende EU-weite Regelung kann zu einer Absenkung des Schutzniveaus in den Mitgliedstaaten führen. Auch soweit es um den Schutz wichtiger – auch über den engen Bereich der „nationalen Sicherheit“ hinausgehender – grundlegender nationaler Interessen wie der öffentlichen Sicherheit, der Landesverteidigung oder der öffentlichen Ordnung geht, sollten die Mitgliedstaaten die Nutzung von Cloud-Diensten auch an strengere (nationale) Voraussetzungen und Souveränitätsanforderungen knüpfen bzw. diese beibehalten dürfen. Soweit bestehende nationale Schemata mit einem von der EU beschlossenen EUCS überlappen, müssten die Mitgliedstaaten ihre Schemata aber so anpassen, dass sie nur noch für die ihnen nach den oben

[142] EuGH, Urteil vom 29. 1. 2008, Rs. C-275/06 – promusicae, ECLI:EU:C:2008:54, Rn. 49 ; vgl auch Schill, S./Krenn, C, in: Grabitz, E./ Hilf, M./Nettesheim, M., Art. 4 EUV Rn. 42.
[143] Art. 4 Abs. 2 lit a), Art. 2 Abs. 2 des Vertrags über die Arbeitsweise der EU (AEUV).
[144] Art. 2 Abs. 2 S. 2 AEUV; vgl. auch Nettesheim, M., in: Grabitz, E./Hilf, M./Nettesheim, M., Art. 2 AEUV Rn. 25.
[145] Nettesheim, M., a.a.O.

genannten Regeln und insbesondere dem Verhältnismäßigkeitsprinzip vorbehaltenen Regelungsbereiche gelten.

Wie oben bereits ausgeführt, dürfen die Mitgliedstaaten aber auch zum Zwecke des in ihrer alleinigen Kompetenz verbleibenden Schutzes der nationalen Sicherheit (ergänzende) Souveränitätsanforderungen mit ggf. höherem Schutzniveau vorsehen oder beibehalten, die dem Schutz ihrer nationalen Sicherheit dienen. Diese Anforderungen dürften sie grundsätzlich auch in ein (ergänzendes) nationales Schema für die Cybersicherheitszertifizierung aufnehmen. Dies spiegelt sich auch in Erwägungsgrund 94 des CSA wider, der anerkennt, dass die Mitgliedstaaten „aus Gründen der nationalen Cybersicherheit“[146] ausnahmsweise nationale Cyberzertifizierungsschemata einführen oder beibehalten dürfen.

3.5.3 Überschneidungen und Vereinbarkeit mit dem EU Data Act

Der im Dezember 2023 in Kraft getretenen „EU-Data Act“ (s. cep**Analyse**)[147] enthält bereits einige Anforderungen, die einigen Souveränitätskriterien sehr ähneln, die im Zusammenhang mit dem EUCS diskutiert werden. So verpflichtet er Anbieter von Datenverarbeitungsdiensten – darunter fallen etwa Cloud- und Edge-Dienste – erstens dazu, „angemessene“ und „zumutbare“ technische, organisatorische und rechtliche Maßnahmen zu ergreifen (etwa vertragliche Vereinbarungen zu treffen), um einen unrechtmäßigen staatlichen Zugang durch Drittstaatsbehörden zu in der EU gespeicherten nicht-personenbezogenen Daten oder deren Übermittlung an Drittstaatsbehörden zu verhindern, wenn dieser Zugang bzw. diese Übermittlung dem EU- oder nationalem Recht widersprechen würde.[148] Zweitens sieht er vor, dass Urteile und Entscheidungen von Gerichten oder Verwaltungsbehörden aus Drittstaaten, die einen Anbieter von Datenverarbeitungsdiensten auffordern, nicht-personenbezogene Daten zu übermitteln oder Zugang zu diesen zu gewähren, in der EU nur anerkannt oder vollstreckt werden dürfen, wenn dies von einer rechtskräftigen internationalen Übereinkunft wie z.B. einem Rechtshilfeabkommen gedeckt ist. Diese Regelung entspricht Art. 48 der Datenschutzgrundverordnung (DSGVO)[149], der das Gleiche für den Fall regelt, dass ein Urteil oder eine Entscheidung eines Drittstaats von einem Verantwortlichen oder Auftragsverarbeiter – hier ebenfalls der Cloud-Dienste-Anbieter – die Übermittlung oder Offenlegung personenbezogener Daten verlangt. Beide Regelungen verbieten Cloud-Dienste-Anbietern Datenübermittlungen aus der EU heraus allein aufgrund einseitiger

[146] Ob der Begriff der „nationalen Cybersicherheit“ als Unterbereich der „nationalen Sicherheit“ anzusehen ist, ist allerdings unklar. Der Begriff wird lediglich in Erwägungsgrund 94 erwähnt und im CSA nicht näher definiert.

[147] Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung).

[148] Art. 32 Abs. 1 Verordnung (EU) 2023/2854 (EU Data Act). Bei diesen Maßnahmen handelt es sich um die Umsetzung von Schutzvorkehrungen durch Cloud-Dienste-Anbieter. Diese Schutzvorkehrungen sollen es EU-Bürgern, der öffentlichen Hand und Unternehmen ermöglichen, die Kontrolle über ihre Daten zu behalten und EU-Standards im Hinblick auf „Sicherheit, Datenschutz und Privatsphäre sowie Verbraucherschutz“ zu wahren. Cloud-Dienste-Anbieter müssen unrechtmäßige staatliche Zugänge aus Drittländern, sofern zumutbar, gegebenenfalls durch „die Verschlüsselung von Daten, häufige Audits, die Überprüfung der Einhaltung der einschlägigen Systeme für die Sicherheitszertifizierung und die Änderung der Unternehmenspolitik“ zu verhindern suchen [Erwägungsgrund 102 Data Act].

[149] Der Europäische Datenschutzausschuss (EDSA) hat am 3. Dezember 2024 Leitlinien zu Art. 48 DSGVO veröffentlicht. Die Leitlinien 02/2024 sollen Unternehmen und Organisationen helfen, eine Entscheidung darüber zu treffen, ob und unter welchen Bedingungen sie personenbezogene Daten rechtmäßig an Behörden aus Drittländern übermitteln dürfen, wenn sie dazu aufgefordert werden. In den Leitlinien beleuchtet der EDSA auch mögliche Rechtsgrundlagen nach Art. 6 DSGVO sowie die erforderlichen Gründe nach Art. 44 ff. DSGVO für eine solche Datenübermittlung. Zugleich können alle Interessenträger und Bürger aktuell noch bis zum 27. Januar 2025 im Rahmen einer öffentlichen Konsultation zu den Leitlinien Stellung nehmen.

Entscheidungen eines Drittstaates und sollen so völkerrechtswidrige extraterritoriale Zugriffe unmittelbar bei Privaten unter Umgehung oder Auslassung staatlicher Wege bzw. ohne rechtstaatliche Verfahrensgarantien verhindern.[150] Der Data Act geht aber noch über die DSGVO hinaus, als er den Anbietern auch für den Fall, dass keine internationale Übereinkunft vorliegt, Regeln für die Zugangsgewährung bzw. die Übermittlung an Drittstaaten vorgibt.[151] Drittens verpflichtet der Data Act Anbieter von Datenverarbeitungsdiensten, ihre Kunden über ein etwaiges Datenzugangsverlangen von Behörden aus Drittstaaten zu informieren, bevor sie dieses erfüllen, außer wenn das Verlangen Strafverfolgungszwecken dient und zur Durchführung wirksamer Strafverfolgungsmaßnahmen erforderlich ist.[152] Viertens müssen sie Transparenz wahren und auf ihren Websites

- Informationen über die Gerichtsbarkeit bereitstellen, der ihre für die Datenverarbeitung errichtete IKT-Infrastruktur unterliegt, und
- eine allgemeine Beschreibung der technischen, organisatorischen und vertraglichen Maßnahmen veröffentlichen, die sie zur Verhinderung des Zugangs durch Drittstaatsbehörden zu in der EU gespeicherten nicht-personenbezogenen Daten oder zur Verhinderung ihrer Übermittlung an Drittstaatsbehörden getroffen haben.[153]

Diese Regelungen – die in der Debatte über Souveränitätsanforderungen oftmals übersehen werden[154] – sind ein weiteres Puzzleteil, das die EU vor unautorisiertem Zugang zu personenbezogenen und nicht-personenbezogenen Daten durch Drittstaatsbehörden schützen soll. Während die Regelungen der DSGVO bereits gelten, werden die Vorgaben des Data Act ab dem 11. September 2025 anwendbar sein. Die EU muss daher darauf achten, dass jegliche künftige Verabschiedung von Souveränitäts- und sonstigen Cybersicherheitsanforderungen, sei es im Rahmen eines EUCS oder durch den EU-Gesetzgeber, den genannten Anforderungen in DSGVO und Data Act nicht widerspricht. Die im EUCS zwischenzeitlich vorgesehenen Souveränitätsanforderungen gehen über die genannten Regelungen im Data Act und der DSGVO hinaus. So regelt der Data Act nicht im Detail, welche technischen, organisatorischen und vertraglichen Maßnahmen der Anbieter treffen muss, sondern erwähnt lediglich allgemeine Beispiele wie Verschlüsselung, Audits und Überprüfungen, während das EUCS hier detailliertere Anforderungen aufstellt. Auch schreibt der Data Act weder eine Datenlokalisierung noch das Erfordernis eines Headquarters in der EU vor. Bei der Ausgestaltung der Anforderungen zur Verhinderung von Zugriffen sollte die EU auf die Erfahrungen betreffend die Wirksamkeit der genannten Regelungen in DSGVO und Data Act zurückgreifen.

3.5.4 Vereinbarkeit mit der Verordnung über den freien Verkehr nicht personenbezogener Daten

Die Verordnung (EU) 2018/1807 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (Free Flow of Data Regulation, s. cep**Analyse**)[155] verbietet den EU-Mitgliedstaaten, Datenlokalisierungsauflagen beizubehalten oder neu zu regeln, soweit diese nicht aus

[150] Zerdick, T., in Ehmann/Selmayr, 3. Auflage 2024, Art. 48 Rn. 1 (für die DSGVO).
[151] Art. 32 Abs. 3 der Verordnung (EU) 2023/2854 (EU Data Act).
[152] Art. 32 Abs. 5 sowie Erwägungsgrund 101 und 102 der Verordnung (EU) 2023/2854 (EU Data Act).
[153] Art. 28 Abs. 1 Verordnung (EU) 2023/2854 (EU Data Act).
[154] Goyet, M., Europäische Kommission, Deputy Head of Unit – Cloud and Software, auf einer Veranstaltung des Forums Europe zum European Sovereign Cloud Day, abrufbar hier.
[155] Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union; näher hierzu Hoffmann, A. / Eckhardt, P., Freier Verkehr nicht personenbezogener Daten, s. cep**Analyse** 33/2017.

Gründen der öffentlichen Sicherheit gerechtfertigt und verhältnismäßig sind.[156] Datenlokalisierungsauflagen in diesem Sinne sind nationale Rechts- oder Verwaltungsvorschriften, die vorschreiben, dass Daten im eigenen Mitgliedstaat gespeichert oder verarbeitet werden müssen, oder die die Speicherung oder Verarbeitung von Daten in einem anderen Mitgliedstaat behindern, etwa durch die Pflicht, einen lokalen Anbieter zu nutzen oder eine Genehmigung einzuholen.[157]

Datenlokalisierungsauflagen, die auf der Grundlage des bestehenden Unionsrechts festgelegt wurden, bleiben von diesem Verbot unberührt. Die Verordnung bezweckt aber lediglich, den freien Verkehr nicht-personenbezogener Daten innerhalb der EU (und nicht mit Drittstaaten) durch den Abbau von „Lokalisierungsbeschränkungen" zu verbessern, Rechtsunsicherheit zu beseitigen und so einen wirksam funktionierenden Binnenmarkt für Cloud-Dienstleistungen zu schaffen. Eine Datenlokalisierung in der EU verbietet sie hingegen nicht.

3.5.5 Eingriff in EU-Grundrechte?

Eine Verpflichtung bestimmter wesentlicher, wichtiger bzw. „kritischer" EU-Unternehmen, ausschließlich zertifizierte Cloud-Dienste zu nutzen, könnte die in Art. 16 der EU-Grundrechtecharta verankerte unternehmerische Freiheit dieser Unternehmen einschränken, ihren Cloud-Dienste-Anbieter frei zu wählen. Solange die Zertifizierung freiwillig bleibt, steht es den Unternehmen jedoch frei, alternative – nicht nach dem EUCS zertifizierte – Anbieter zu nutzen. Sofern die Zertifizierung künftig – für einzelne Unternehmen oder Einrichtungen – zur Pflicht werden soll, müsste genau geprüft werden, inwieweit der in der Pflicht zur Nutzung zertifizierter Cloud-Dienste liegende Eingriff gerechtfertigt werden kann. Dies setzt laut der Rechtsprechung des EuGH nach Art. 52 Abs. 1 der EU-Grundrechtecharta voraus, dass der Eingriff auf Basis einer gesetzlichen, rechtsverbindlichen Grundlage erfolgt, d.h. auf einer vom EU-Gesetzgeber erlassenen Bestimmung beruht.[158] Zwar hat der EuGH eine Durchführungsverordnung – wie sie auch bei Verabschiedung des EUCS durch die Kommission vorläge – als „Gesetz" i.S.d. Art. 52 Abs. 1 GRCh eingestuft.[159] Eine Durchführungsverordnung reicht aber nicht aus, wenn die fraglichen Vorschriften Eingriffe in die Grundrechte der betroffenen Personen in einem Umfang erlauben, der ein Tätigwerden des Unionsgesetzgebers erforderlich macht. Dies ist laut dem EuGH der Fall, wenn der Erlass der Vorschriften politische Entscheidungen erfordert, die eine Abwägung der widerstreitenden Interessen auf der Grundlage einer Beurteilung zahlreicher Gesichtspunkte einschließen und daher in die Zuständigkeit des Unionsgesetzgebers fallen.[160]

Souveränitätsanforderungen mit einer hohen Eingriffstiefe wie etwa das Erfordernis einer strikten Datenlokalisierung in der EU bzw. die Nutzung ausschließlich von Anbietern mit Hauptverwaltung in der EU müssten daher – soweit sie nicht bereits im Data Act oder in der DSGVO vorgesehen oder vom CSA oder sonstigem EU-Recht gedeckt sind – vom EU-Gesetzgeber und nicht allein von der Kommission geregelt werden. Ist dies der Fall oder erfolgt zukünftig, wäre weiter zu prüfen: Die Nutzungspflicht bzw. der Eingriff dient legitimen Zwecken, nämlich etwa der Aufrechterhaltung der Funktionsfähigkeit der von wichtigen oder kritischen Unternehmen und Einrichtungen betriebenen IKT-Infrastrukturen, und könnte daher nach Art. 52 der EU-GRCh gerechtfertigt sein. Hierzu müsste die Nutzungspflicht jedoch zum Schutz dieser Interessen geeignet und erforderlich sein. Die Souveränitätsanforderungen

[156] Art. 1 Abs. 1 Verordnung (EU) 2018/1807.
[157] Vgl. Hoffmann, A./ Eckhardt, P., a.a.O., S. 2.
[158] EuGH, Urteil vom 4. Mai 2016, Rs. C-547/14 – Philipp Morris, ECLI:EU:C:2016:325, Rn. 150.
[159] EuGH, Urteil vom 9. November 2010, verb. Rs. C-92/09 und C-93/09 – Schecke, ECLI:EU:C:2010:662, Rn. 66; siehe auch Jarass, H., Charta der Grundrechte der EU, 4. Auflage 2021, Art. 52 Rn. 25.
[160] EuGH, Urteil vom 5. September 2012, Rs. C-355/10 – EP ./. Rat, ECLI:EU:C:2012:516, Rn. 77, 76, 84.

müssen also zunächst geeignet sein, die in sie gesetzten Ziele tatsächlich zu erreichen – z.B. sensible Daten vor unerwünschten Zugriffen aus Drittstaaten zu schützen oder für eine bessere Durchsetzung von EU-Recht gegenüber Cloud-Dienste-Anbietern zu sorgen. Hiervon dürfte auszugehen sein, soweit die Souveränitätsanforderungen dazu beitragen, die Rechtsdurchsetzung zu erleichtern und ungerechtfertigte Zugriffe auf die Daten zumindest zu erschweren, auch wenn solche Zugriffe u.U. trotz Erfüllung der Souveränitätsanforderungen letztlich nicht vollständig vermieden werden können.

Die Souveränitätskriterien müssten zudem erforderlich sein, d.h. es darf kein milderes Mittel geben. Im Rahmen dieser Verhältnismäßigkeitsprüfung sind die widerstreitenden Interessen unter Einbeziehung aller relevanten Aspekte des Einzelfalls gegeneinander abzuwägen, darunter einerseits die Sensibilität und Schutzwürdigkeit der Daten und Infrastrukturen und andererseits die Sinnhaftigkeit der Anforderungen sowie die Nachteile, welche EU-Unternehmen aus der Pflicht erwachsen, einen auf einer bestimmten Vertrauenswürdigkeitsstufe zertifizierten Cloud-Dienst nutzen zu müssen. Dies wird für jede Souveränitätsanforderung einzeln als auch in ihrer Gesamtheit zu prüfen sein. So könnte eine Pflicht zur Nutzung von Anbietern, die ihre Daten ausschließlich in der EU speichern, ihre Hauptverwaltung dort haben und keinerlei Verbindung zu einem US-Unternehmen aufweisen, unverhältnismäßig sein, soweit wenig sensible Daten verarbeitet werden und die Verarbeitung von sensiblen und nicht sensiblen Daten getrennt bzw. sinnvoll trennbar ist. Zu prüfen ist in diesem Zusammenhang etwa auch, wie realistisch die Annahme ist, dass in der EU tätige Cloud-Anbieter sich durch die Anforderungen, die ihre Immunität vom Drittstaatsrecht sicherstellen sollen, tatsächlich dem Zugriff durch Drittstaatsbehörden werden entziehen können, also durch sie in der Praxis faktische „Immunität“ vom Drittstaatsrecht erreicht werden kann. Auf die USA bezogen wird dies nicht zuletzt davon abhängen, wie die US-Gerichte die Versuche der Unternehmen beurteilen, sich von der US-Gerichtsbarkeit bzw. vom US CLOUD Act[161] zu lösen[162], und welche Konsequenzen die USA hieraus ziehen bzw. welche Gegenmaßnahmen sie hier ggf. erwägen könnten, wenn ihre Gesetze nicht die gewünschte Wirkung erzielen.

3.5.6 Potenzielle Konflikte mit dem internationalen Handelsrecht

Die EU und ihre einzelnen Mitgliedstaaten sind Mitglied der Welthandelsorganisation (WTO); dabei vertritt die EU die im Zuge der Gemeinsamen Handelspolitik abgestimmten Interessen aller Mitgliedstaaten.[163] Bei Mehrheitsentscheidungen übt die EU das Stimmrecht für alle Mitgliedstaaten aus und verfügt insoweit über 27 Stimmen, wobei die Stimme der EU als selbständiges WTO-Mitglied entfällt. Das WTO-Recht beruht hauptsächlich auf drei Säulen. Kernstück des Welthandelsrechts ist das Allgemeine Zoll- und Handelsabkommen (General Agreement on Tariffs and Trade, GATT)[164]; es enthält die für den internationalen Warenhandel grundlegenden Regelungen über den Abbau von Zöllen und die Beseitigung sonstiger, nichttarifärer Handelsbarrieren. In seinen Anwendungsbereich fallen „Waren“, „Güter“, „Erzeugnisse“ und „Produkte“ und damit alle physisch greifbaren Sachen, die Gegenstand von Handelsgeschäften sein können. Davon abzugrenzen ist der Handel mit Dienstleistungen, der unter

[161] Gesetz über die Klarstellung der Nutzung von Daten im Ausland (US Clarifying Lawful Overseas Use of Data Act), H.R. 4943, Text siehe hier. Der US CLOUD Act verpflichtet Cloud-Dienste-Anbieter mit Verbindungen zu den USA unter bestimmten Bedingungen auch zur Offenlegung von Kommunikationsdaten, die außerhalb der Vereinigten Staaten gespeichert werden, sich aber unter ihrer „Kontrolle“ befinden. Näher dazu Hoffmann, A. (2021), Unzulässigkeit der Datenübermittlung in die USA, s. cep**Studie**.

[162] Vgl. auch Propp, K. (2022), European Cybersecurity Regulation Takes a Sovereign Turn, abrufbar hier.

[163] Miederer, K., Der Beitritt zur Welthandelsorganisation und zur Europäischen Union, Ein Vergleich der angewandten Verfahren und Kriterien, Universität Bremen 2002.

[164] WTO, General Agreement on Tariffs and Trade, unterzeichnet am 30. Oktober 1947, in Kraft getreten am 1. Januar 1948, in der Fassung von 1994, abrufbar hier.

den Anwendungsbereich des Allgemeinen Dienstleistungsabkommens (General Agreement on Trade in Services, GATS)[165] fällt, welches die zweite[166] Säule des WTO-Rechts bildet.[167] Zur Lösung von Handelsstreitigkeiten bietet die WHO ein Streitbeilegungssystem. Die Streitbeilegung obliegt hierbei zunächst dem Dispute Settlement Body als Streitbeilegungsgremium; die Mitgliedstaaten können aber die Errichtung eines Streitschlichtungspanels (Dispute Panels) fordern.[168]

Fallen Souveränitätsanforderungen unter ein Verbot des GATS?

Das GATS deckt mit wenigen Ausnahmen alle Dienstleistungen ab.[169] Cloud Computing fällt unter die Kategorie „Computer- und verwandte Dienstleistungen" und damit ausdrücklich unter das GATS.[170] Das GATS gilt für „alle Maßnahmen von Mitgliedern, die den Handel mit Dienstleistungen beeinflussen" (Art. 1 GATS). Es soll die Grundsätze des GATT auf den Bereich der Dienstleistungen übertragen. Nicht nur Zölle oder Kontingente, sondern auch Marktzugangsbeschränkungen und Regelungen betreffend die Qualifikation von Dienstleistungserbringern gelten somit seither als Handelsbeschränkungen.[171]

Zu den wesentlichen Prinzipien des GATT gehört der Grundsatz der Inländerbehandlung.[172] Dieser verpflichtet die Mitgliedsländer, ausländische Waren, sobald sie importiert wurden, genauso zu behandeln wie inländische Waren.[173] Als Teil des allgemeinen Diskriminierungsverbots des GATT dient er der Schaffung gleicher Wettbewerbsbedingungen und soll zugleich Protektionismus verhindern.[174] Entsprechend verbietet der Grundsatz der Inländerbehandlung im GATS die Diskriminierung einer ausländischen Dienstleistung im Vergleich zu einer gleichartigen inländischen Dienstleistung.[175] Eine Diskriminierung liegt vor, wenn die fraglichen Maßnahmen die Wettbewerbsbedingungen zugunsten inländischer Dienstleistungserbringer verändern. Hiervon wird nicht nur die rechtliche, sondern grundsätzlich auch die faktische Schlechterstellung ausländischer Anbieter erfasst.[176] Für das öffentliche Beschaffungswesen besteht im Rahmen der WTO ein separates Übereinkommen, weil die öffentliche Beschaffung ausdrücklich von den wichtigsten Liberalisierungen des GATT und des GATS ausgenommen ist. Das sogenannte Abkommen über das öffentliche Beschaffungswesen [Government Procurement Agreement (GPA)][177] schreibt bei öffentlichen Aufträgen ebenfalls die Inländerbehandlung und Nichtdiskriminierung vor. Als „plurilaterales" Abkommen gilt es jedoch nicht für alle WTO-Mitglieder, sondern nur für die Unterzeichner, darunter die EU, USA und Japan.[178] Die EU hat u.a. im Sektor

[165] WTO, General Agreement on Trade in Services (GATS), abrufbar hier.
[166] Die dritte Säule bildet das – hier nicht relevante TRIPS-Abkommen Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), abrufbar hier.
[167] Deutscher Bundestag (2019), Gutachten des Wissenschaftlichen Dienstes, Sachstand, Zur Geltendmachung nationaler Sicherheitsinteressen beim Aufbau des 5G-Netzes, abrufbar hier.
[168] Näher dazu WTO, Dispute Settlement System Training Module, Ziffern 3.1 und 3.3. Vgl. auch Wikipedia, Dispute Settlement Body.
[169] World Trade Organization, Services: Services Sectors, siehe hier.
[170] World Trade Organization, Services: Sector by Sector, Computer and related services, siehe hier; differenzierend nach Funktionalitäten des Cloud-Dienstes Willemyns, I. (2008), GATS Classification of Digital Services - Does 'The Cloud' Have a Silver Lining?, siehe hier. Weil Cloud-Dienste Telekommunikationsnetze nutzen, können u.U. auch die Verpflichtungen und Marktöffnungen der EU in diesem Bereich relevant sein.
[171] Hofmann, R., Skript Internationales Wirtschaftsrecht WS 2013/14, Teil 3, Das WTO/GATT-System, § 8 Grundprinzipien des GATS, S. 2, abrufbar hier.
[172] Art. III GATT 1994.
[173] JuraForum, GATT: Definition & Bedeutung im internationalen Handel und Wirtschaftsrecht, siehe hier.
[174] Hofmann, R., Teil 3 § 7, a.a.O., S. 3.
[175] Fischer, K. (2022), Die WTO und der Dienstleistungshandel, siehe hier.
[176] Fischer, K. (2022), a.a.O., vgl. auch Hofmann, R., Teil 3 § 8, a.a.O., S. 6.
[177] Die derzeit gültige überarbeitete Fassung des Abkommens aus dem Jahr 2012 ist hier abrufbar unter.
[178] Bauer, N. (2022), WTO und öffentliche Beschaffung, abrufbar hier.

Telekommunikation Ausnahmen festschreiben lassen.[179] Unter Berufung auf die Inländerbehandlung hatte etwa die US- Botschafterin bei der WTO Bedenken geäußert und die EU zu einer Überprüfung des EUCS aufgerufen. Die EU habe im Rahmen des GPA Verpflichtungen für Cloud-Dienste übernommen und sei daher verpflichtet, einen diskriminierungsfreien Zugang zu den betroffenen Beschaffungen zu gewährleisten.[180] Da das GPA im Übrigen ähnliche Grundsätze und Ausnahmen regelt[181] wie das GATT und das GATS, wird im Rahmen dieses cep**Input** nicht separat darauf eingegangen.

Sie verbietet die Diskriminierung einer ausländischen Dienstleistung im Vergleich zu einer gleichartigen inländischen Dienstleistung. Entsprechendes gilt für die Erbringer von Dienstleistungen. Eine Diskriminierung liegt vor, wenn eine oder mehrere Maßnahmen Wettbewerbsbedingungen verändern, und zwar zu Gunsten inländischer Dienstleistungen bzw. inländischer Dienstleistungserbringer.

Anders als beim GATT gilt der Grundsatz der Inländerbehandlung im Rahmen des GATS nicht generell für alle WTO-Mitgliedstaaten. Das GATS unterscheidet insoweit zwischen allgemeinen, für alle WTO-Mitglieder geltenden Pflichten in Teil II[182] und „spezifische(n)“ Verpflichtungen in Teil III, welche nur für diejenigen Mitgliedstaaten gelten, die sich explizit dazu verpflichtet haben. Hierzu gehören der Abbau von Marktzugangsbeschränkungen (Art. XVI)[183] und der Grundsatz der Inländerbehandlung (Art. XVII).[184] Marktzugang und Inländerbehandlung gelten daher nur im Rahmen der konkreten Verpflichtungen, die die Länder in ihren Listen ("schedules") eingegangen sind. Einen Anspruch auf Marktzugang, d.h. darauf, den Markt des anderen Mitgliedstaates (hier der EU) zu erschließen, besteht daher nur, soweit dies in den genannten Länderlisten geregelt ist.[185]

Inwieweit die EU und die EU-Mitgliedstaaten im Rahmen des GATS allgemeine und sektorspezifische Verpflichtungen übernommenen haben, die auch für Cloud-Dienste als „neuere“ Dienstleistungsart gelten, erfordert eine komplizierte Prüfung[186], die an dieser Stelle nicht vorgenommen wird. Gleiches gilt für die Frage, welche möglicherweise relevanten Ausnahmen von den Verpflichtungen explizit in die Listen aufgenommen wurden. Für die Zwecke dieses cep**Input** soll daher vorbehaltlich einer näheren Prüfung unterstellt werden, dass die EU bzw. ihre Mitgliedstaaten im Rahmen des GATS Verpflichtungen übernommen haben, die sie grundsätzlich zur Marktöffnung und Inländerbehandlung für Cloud-Dienste-Anbieter verpflichten.

Fraglich ist, ob Souveränitätsanforderungen, die Cloud-Dienste-Anbieter zur Datenlokalisierung in der EU verpflichten oder ein Tätigwerden an einen Haupt(verwaltungs)sitz in der EU knüpfen, mit der angestrebten Liberalisierung des Dienstleistungshandels im Widerspruch stehen, weil sie möglicherweise den Zugang von Drittstaatsanbietern zum EU Cloud-Markt zu Unrecht beschränken oder im Vergleich zu europäischen Anbietern schlechterstellen. Dieser Ansicht sind 26 Industriegruppen, die im Juni 2024

---

[179] Siehe Schlussbericht der Enquete-Kommission „Globalisierung der Weltwirtschaft – Herausforderungen und Antworten“, BT-Drucks. 14/9200 vom 12. Juni 2002, Ziffer 3.3.3.1.7, abrufbar hier.

[180] Pagán, M. (2023), U.S. Opening Remarks at the Trade Policy Review of the European Union, abrufbar hier; vgl. auch Propp (2023), Oceans apart: The EU and US Cybersecurity Certification Standards for Cloud Services, abrufbar hier.

[181] So sieht das Übereinkommen über das öffentliche Beschaffungswesen in Art. III ähnlich gelagerte Ausnahmen zum Schutz der öffentlichen Ordnung, des Lebens und der Gesundheit von Menschen sowie der wesentlichen Sicherheitsinteressen vor. Auf diese Ausnahmen wird unten im Rahmen des GATS noch näher eingegangen.

[182] Zu diesen gehören etwa der Grundsatz der Meistbegünstigung (Art. II GATS) und Transparenzpflichten (Art. III GATS).

[183] Text abrufbar hier.

[184] Text abrufbar hier. Vgl. dazu Hofmann, R., Teil 3 § 8, a.a.O., S. 2.

[185] Die Listen sind also für die Frage des Marktzugangs von ganz entscheidender Bedeutung, vgl. Fischer, K. (2022), Die WTO und der Dienstleistungshandel, vgl. hier.

[186] Gut veranschaulicht bei Ungphakorn, P. (2021), Technical note: what are schedules of commitments in services?, Trade β Blog, siehe hier.

In einem gemeinsamen Brief[187] an die EU-Mitgliedstaaten erklärten, die zwischenzeitlich im EUCS geregelten strengen Souveränitätsanforderungen führten zu einer Diskriminierung der großen US-Cloud-Dienste-Anbieter wie Amazon, Alphabet (Google) und Microsoft.[188] Bereits im Mai hatten die amerikanische Handelskammer bei der EU sowie zwölf weitere Industrieverbände in einer gemeinsamen Erklärung darauf hingewiesen, dass die Anforderungen an die Eigentumsverhältnisse von Unternehmen, die Datenlokalisierung und die Immunität gegen Nicht-EU-Recht die große Mehrheit der außereuropäischen Cloud-Dienste-Anbieter daran hindern würden, ihre Dienste Kunden in der EU anzubieten, die auf der höchsten Vertrauenswürdigkeitsstufe zertifizierte Cloud-Dienste in Anspruch nehmen wollen.[189] Auch andere Stimmen weisen darauf hin, dass verpflichtende Maßnahmen zur Datenlokalisierung den Datenfluss behindern und somit Handelshemmnisse darstellen. Denn sie erhöhten die Befolgungskosten für ausländische Dienste-Anbieter und begrenzten deren Marktzugangsmöglichkeiten. Gleichzeitig hätten Endverbraucher und Unternehmen in der EU, die Cloud-Dienste nutzen (möchten), einen eingeschränkten Zugang zu wettbewerbsfähigen ausländischen Diensten und verlören dadurch u.a. bedeutende Geschäftsmöglichkeiten.[190]

Auf der anderen Seite führen Regierungen zunehmend starke politische Argumente an, um die Datenlokalisierung zu rechtfertigen. Sie propagieren, wie China und Russland, entweder allgemein die Notwendigkeit einer starken souveränen Kontrolle oder argumentieren spezifischer, dass ihre Maßnahmen etwa zur Gewährleistung von Datenschutz und Netzsicherheit, zur Verhinderung von Cyberkriminalität, zur Unterstützung inländischer Strafverfolgung und zum Schutz des geistigen Eigentums erforderlich seien. Dass sich hinter diesen Maßnahmen oft zumindest auch protektionistische Gründe verbergen, geben die meisten Länder nur selten zu.[191]

Rechtfertigung durch Ausnahmetatbestände des GATS?

Das GATS sieht verschiedene **Ausnahmetatbestände** vor, die es den Mitgliedstaaten erlauben, unter bestimmten Umständen von seinen Prinzipien, wie dem Gebot des Marktzugangs und der Nichtdiskriminierung, abzuweichen. Sie sollen es den Mitgliedstaaten ermöglichen, trotz der grundsätzlichen Beschränkung ihres Handlungsspielraums durch ihre handelsrechtlichen Verpflichtungen den Schutz wichtiger Güter sicherstellen zu können.[192] Allerdings stammt das GATS aus der Zeit vor dem Internet und es bestehen daher Rechtsunsicherheiten, inwieweit sich seine Regelungen zur Lösung der Herausforderungen des digitalen Zeitalters heranziehen lassen.[193]

---

[187] Zu den Unterzeichnern des Briefs gehörten die American Chamber of Commerce in der Tschechischen Republik, Estland, Finnland, Italien, Norwegen, Rumänien und Spanien und die „European Payment Institutions Federation (EPIF)“ sowie der Bundesverband deutscher Banken, vgl. Chee, F. (2024), EU cybersecurity label should not discriminate against Big Tech, European groups say, siehe hier.

[188] Chee, F., (2024), a.a.O.

[189] Joint industry statement on the need for a swift adoption of the EU Cybersecurity Certification Scheme for Cloud Services without sovereignty requirements, siehe hier.

[190] So – allgemein für digitale Dienste – Mishra, N. (2019), Privacy, Cybersecurity and GATS Article XIV: A New Frontier for Trade and Internet Regulation?, S. 3, 6f., vgl. hier.

[191] Mishra, N. (a.a.O.), S. 8.

[192] Deutscher Bundestag (2019), Gutachten des Wissenschaftlichen Dienstes, S. 6, siehe hier zum GATT; dies gilt auch für das GATS.

[193] Näher zu dieser Problematik Mishra, N. (2019), a.a.O., S. 13. Insbesondere gibt es bislang keine Auslegungshilfe für digitale Handelsverpflichtungen, da es auch im Rahmen der letzten Präferenzhandelsabkommen keine diesbezüglichen Streitigkeiten gegeben hat, vgl. Burri, M. / Kugler, K., Regulatory autonomy in digital trade agreements, Zeitschrift für Internationales Wirtschaftsrecht, 2024, S. 397 (410), vgl. hier.

Souveränitätsanforderungen, die zum Schutz der Daten, der Privatsphäre und der Cybersicherheit dienen sollen, könnten zunächst unter die **allgemeinen Ausnahmen des GATS** fallen.[194] Danach dürfen die Mitgliedstaaten unter bestimmten Voraussetzungen Maßnahmen ergreifen, die erforderlich sind, um die öffentliche Ordnung aufrechtzuerhalten (Art. XIV Buchstabe a GATS). Sie dürfen auch erforderliche Maßnahmen ergreifen, um die Einhaltung von Gesetzen sicherzustellen, die die Sicherheit oder den Schutz der Persönlichkeit bei der Verarbeitung und Weitergabe personenbezogener Daten und zum Schutz der Vertraulichkeit persönlicher Aufzeichnungen und Konten gewährleisten sollen (Artikel XIV Buchstabe c GATS). Datenschutz wird also ausdrücklich als ein legitimes Ziel anerkannt. Dies spricht dafür, dass es sich z.B. bei einer Einschränkung auf Standorte in Staaten mit einem angemessenen Datenschutz um eine WTO-kompatible Maßnahme handeln kann. Die Ausnahmeregelung für die öffentliche Ordnung kann jedoch nur geltend gemacht werden, soweit eine tatsächliche und hinreichend schwere Bedrohung eines der grundlegenden Interessen der Gesellschaft vorliegt. Soweit die EU geltend machen kann, dass die Souveränitätsanforderungen grundlegende Interessen der EU-Bürger berühren, könnte Artikel XIV(a) GATS auch zur Rechtfertigung von Cybersicherheitsmaßnahmen herangezogen werden.[195] So könnte er etwa Maßnahmen zur Bekämpfung von Sicherheitsbedrohungen im Internet der Dinge ("IoT") abdecken, die eine "ernsthafte Bedrohung" für die Sicherheit aller mit intelligenten Geräten verbundenen Haushalte darstellen.[196]

Die allgemeinen Ausnahmetatbestände des GATS sollen ein Gleichgewicht zwischen den Verpflichtungen zur Liberalisierung des internationalen Handels und dem nationalen Verständnis eines Mitglieds von Privatsphäre und Cybersicherheit als Ziele der Datenlokalisierungsmaßnahmen schaffen.[197] Welche Maßnahmen hierzu jedoch im Einzelnen „erforderlich“ sind, lässt sich nur durch eine schwierige Abwägung zwischen diesen widerstreitenden Zielen und einer Bewertung komplexer technischer Fragen ermitteln.[198] „Erforderlich“ bedeutet, dass keine weniger handelsbeschränkende Alternative „vernünftigerweise verfügbar“ sein darf, die denselben Zweck erfüllt. Die Abwägung wird dadurch verkompliziert, dass Lokalisierungsmaßnahmen oft mehrere Ziele verfolgen und/oder sowohl die Privatsphäre schützen als zugleich auch die einheimische Digitalwirtschaft begünstigen können. Hinter legitimen Gründen können zudem protektionistische Absichten verborgen sein.[199] Die Berufung auf die Ausnahme darf aber nicht missbräuchlich sein, d.h. die Maßnahmen müssen in „gutem Glauben“[200] kohärent um- und durchgesetzt werden und dürfen keine willkürliche oder ungerechtfertigte Diskriminierung oder versteckte Handelsbeschränkung darstellen.[201] Sie dürfen also nicht in erster Linie protektionistischen Zwecken dienen.

Zwar ist die Gewährleistung des freien Datenflusses für die Nutzung des Internets als Plattform für den Austausch von digitalen Diensten wichtig. Auf der anderen Seite sind Datenschutz und Cybersicherheit zugleich grundlegende Voraussetzungen für die Aufrechterhaltung der Stabilität des Internets und die Ermöglichung eines vertrauenswürdigen Umfelds für den grenzüberschreitenden Datenverkehr und

[194] Mishra, N. (2019), a.a.O., S. 12f.
[195] Burri, M. / Kugler, K., Regulatory autonomy in digital trade agreements, Zeitschrift für Internationales Wirtschaftsrecht, 2024, S. 397 (*413*), vgl. hier.
[196] Mishra, N. (2019), a.a.O., S. 17.
[197] Mishra, N. (2019), Privacy, Cybersecurity and GATS Article XIV: A New Frontier for Trade and Internet Regulation?, S. 5, vgl. hier.
[198] Vgl. Mishra, N. (2019), a.a.O., S. 12, 30.
[199] Mishra, N. (2019), a.a.O., S. 3.
[200] Mishra, N. (2019), a.a.O., S. 25.
[201] Burri, M. / Kugler, K., Regulatory autonomy in digital trade agreements, Zeitschrift für Internationales Wirtschaftsrecht, 2024, S. 397 (*414*), vgl. hier.

werden daher zunehmend ebenfalls als Voraussetzung für die Erleichterung des digitalen Handels anerkannt.[202] Einige Experten gehen daher davon aus, dass ein WTO-Panel diesen Zielen wegen ihrer strategischen Bedeutung und der Risiken im Falle ihres Fehlens in einem Handelsstreit über Datenlokalisierung hohe Priorität einräumen dürfte.[203] Eine Datenlokalisierungsmaßnahme könne etwa gerechtfertigt sein, wenn ein Land die Übermittlung von Daten in Länder mit einer sehr schlechten Erfolgsbilanz im Bereich der Cybersicherheit oder des Datenschutzes verhindere, z. B. wenn Regierungen dafür bekannt seien, dass sie Unternehmen zur Herausgabe von Daten zwingen.[204] Umgekehrt könnten bestimmte Formen der Lokalisierung unnötig sein, wenn weniger sensible, nicht-personenbezogene oder anonymisierte Datensätze betroffen seien oder wenn die einem digitalen Dienst zugrunde liegende Technologie sehr sicher und robust sei.[205] Andere Autoren weisen darauf hin, dass die Erfüllung der Voraussetzungen der – eng auszulegenden – GATS-Ausnahmen eine relativ hohe Hürde für WTO-Mitglieder darstellen und die „Erfolgsquote" für eine Berufung auf die Ausnahmen gering sei. Allerdings werden Beschwerden i.d.R. nur dann erhoben, wenn die Erfolgsaussichten hierfür hoch sind. Ob die EU-Souveränitätskriterien tatsächlich Gefahr laufen, vor einem Panel angefochten zu werden, ist aber offen und wird z. T. als eher unwahrscheinlich erachtet.[206] Darauf verlassen kann sich die EU aber nicht.

In jedem Fall haben die Panels bei der Beurteilung der Rechtmäßigkeit von Datenlokalisierungsmaßnahmen einen Ermessensspielraum.[207] Bislang gibt es auch keine Rechtsprechung eines WTO-Panels zu der Ausnahme zum Schutz der Privatsphäre/Datenschutz gemäß Artikel XIV lit. c) GATS[208], die diesen Ermessensspielraum einschränken könnte. Unter den WTO-Mitgliedern besteht nach wie vor kein Konsens über die Rolle von Cybersicherheit und Datenschutz im internationalen Handelsrecht. Zudem fehlt es an spezifischen internationalen Gesetzen, Normen oder Standards zur Cybersicherheit und zum Schutz der Privatsphäre. Fachleute sind im Hinblick auf die wirksamsten Standards für Datenschutz und Cybersicherheit geteilter Meinung. Daher ist die Fähigkeit der WTO-Tribunale, einen Ausgleich zwischen Handelsliberalisierung und legitimen nationalen Interessen zu finden, nach Ansicht von Experten begrenzt und die Panels werden bei einer möglichen Entscheidung über die Legitimität solcher Maßnahmen an Grenzen stoßen.[209]

Neben den allgemeinen Ausnahmen sieht das GATS zudem **Ausnahmen zum Schutz nationaler Sicherheitsinteressen** vor (Art. XIV bis GATS).[210] Danach hindern die GATS-Verpflichtungen die Mitgliedstaaten nicht daran, Auskünfte zu verweigern, deren Preisgabe „nach ihrer Auffassung" ihren „wesentlichen Sicherheitsinteressen" zuwiderläuft, sowie Maßnahmen zu treffen, die „nach ihrer Auffassung" zum Schutz ihrer „wesentlichen Sicherheitsinteressen" notwendig sind. Folglich belässt das GATS die Einschätzungsprärogative, ob wesentliche (nationale) Sicherheitsinteressen bedroht sind, dem

[202] Vgl. Mishra, N. (2019), a.a.O., S. 18, 26.
[203] Vgl. Mishra, N. (2019), a.a.O., S. 18.
[204] Mishra, N. (2019), a.a.O., S. 19.
[205] Mishra S. 27.
[206] Burri, M. / Kugler, K., Regulatory autonomy in digital trade agreements, Zeitschrift für Internationales Wirtschaftsrecht, 2024, S. 397 (419), vgl. hier.
[207] Mishra, N. (2019), a.a.O., S. 28.
[208] Burri, M. / Kugler, K., Regulatory autonomy in digital trade agreements, Zeitschrift für Internationales Wirtschaftsrecht, 2024, S. 397 (*412*), vgl. hier.
[209] Mishra, N. (2019), a.a.O., S. 12f., 29.
[210] Art. XXIII des Abkommens über das öffentliche Beschaffungswesen sieht ebenfalls eine „Sicherheitsausnahme" vor.

jeweiligen WTO-Mitgliedstaat.[211] Der Begriff der „wesentlichen Sicherheitsinteressen“ ist enger als derjenige der „Sicherheitsinteressen“ und bezieht sich auf die wesentlichen Funktionen des Staates in Bezug auf den Schutz seines Territoriums und seiner Bevölkerung vor äußeren Bedrohungen und die Aufrechterhaltung von Recht und öffentlicher Ordnung. Was seine wesentlichen Sicherheitsinteressen sind und welche Maßnahmen notwendig sind, bestimmt jeder Mitgliedstaat zumindest weitestgehend selbst.[212] Dennoch ist die Inanspruchnahme der Sicherheitsausnahme nicht völlig selbstbestimmt.[213] Im Jahr 2019 fällte ein WTO-Panel in einem Streit zwischen Russland und der Ukraine eine wegweisende Entscheidung[214], nachdem sich Russland auf die Sicherheitsausnahme[215] berufen und handelsbeschränkende Maßnahmen zum Schutz seiner nationalen Sicherheit ergriffen hatte.[216] Das Panel entschied, dass Maßnahmen, die WTO-Mitglieder unter Berufung auf die nationale Sicherheit vornehmen, zumindest in objektiver Hinsicht durch die WTO-Streitbeilegungsverfahren überprüfbar sind. Dabei wies es ausdrücklich das Argument Russlands – das in mehreren Fällen auch von den USA geltend gemacht wurde – zurück, dass Maßnahmen zum Schutz wesentlicher Sicherheitsinteressen im alleinigen Ermessen der Mitgliedstaaten lägen und eine Entscheidung eines WTO-Panels hierüber deren nationale Souveränität verletze.[217]

Die Souveränitätsanforderungen der EU müssten somit zumindest aus der Sicht der EU bzw. ihrer Mitgliedstaaten dem Schutz ihrer „wesentlichen Sicherheitsinteressen“ dienen. Einige Experten weisen darauf hin, dass sich die Bedeutung der Cybersicherheit in den letzten Jahren gewandelt hat. Während die Cybersicherheit in erster Linie der Aufrechterhaltung der Funktionsfähigkeit von Netz- und Informationssystemen dient[218], solle das Konzept der Informationssicherheit die Vertraulichkeit (personenbezogener) Daten schützen und ihre Offenlegung verhindern. Die Informationssicherheit falle nicht notwendigerweise in den Bereich der nationalen Sicherheit.[219] Dagegen sei das Streben nach Cybersicherheit in jüngster Vergangenheit immer mehr zu einer Frage der nationalen Sicherheit geworden. Unklar bleibt in jedem Fall, ab welchem Risiko eine Gefahr für welche „wesentliche Interessen“ vorliegt. Darüber hinaus müsste sich die EU bzw. ihre Mitgliedstaaten auf eine Notfallsituation berufen können, um die Sicherheitsausnahme anzuwenden und Maßnahmen ergreifen zu dürfen[220], nämlich entweder, dass sie sich „in Kriegszeiten“ befindet oder einen sonstigen „Notfall“ in den internationalen Beziehungen vorliegt. Einen solchen hatte das Panel im Russland-Ukraine-Fall als "eine Situation eines bewaffneten Konflikts oder eines latenten bewaffneten Konflikts oder einer erhöhten Spannung oder

---

[211] Deutscher Bundestag (2019), Gutachten des Wissenschaftlichen Dienstes, a.a.O., S. 6, zum inhaltlich gleichlautenden Art. XIV bis GATT.

[212] Burri, M. / Kugler, K., a.a.O., S. 422; insoweit ebenso Peng, S., Cybersecurity Threats and the WTO National Security Exceptions, Journal of International Economic Law, 2015, A. 449ff., die dies aus der Auslegung von Text (S. 434) und Kontext (S. 464) des Art. XIV GATS herleitet, vgl. hier.

[213] Siehe dazu bereits Peng, S. (a.a.O.), S. 464, 466f.

[214] WTO Dispute Settlement (DS)512: Russia — Measures Concerning Traffic in Transit, siehe hier.

[215] In diesem Fall Art. XXI GATT, der jedoch in weiten Teilen mit Art. XIV GATS vergleichbar ist.

[216] Hintergrund des Verfahrens war die Blockade des Handels zwischen der Ukraine, Kasachstan und der Kirgisischen Republik im Transit durch Russland als Reaktion auf die Eskalation der Ereignisse in der Ukraine nach den politischen Unruhen im Jahr 2014. Im Ergebnis hielt das Panel die russischen Maßnahmen aber für von der Sicherheitsausnahme gedeckt, vgl. Reinsch, W./ Caporal, J. (2019), Die erste Entscheidung der WTO zur nationalen Sicherheit: Was bedeutet sie für die Vereinigten Staaten?, siehe hier.

[217] Reinsch, W./ Caporal, J. (2019), a.a.O.

[218] Art. 2 Ziffer 1, Verordnung (EU) 2019/881.

[219] Peng, S. (2015), Cybersecurity Threats and the WTO National Security Exceptions, Journal of International Economic Law, 2015, A. 449ff a.a.O., S. 449 (469), vgl. hier.

[220] Art. XIV bis lit. b ii) GATS.

Krise oder einer allgemeinen Instabilität“ definiert, die „einen Staat verschlingt oder umgibt".[221] Ob ein solcher Zustand vorlag, sei durch ein Panel ebenso objektiv überprüfbar wie die Frage, ob die angegriffene Maßnahme „zum Zeitpunkt“ eines solchen Notstands ergriffen wurde und ob sie mit dem genannten Zustand in einem plausiblen Zusammenhang steht.[222] Will sich die EU auf diese Ausnahme berufen, müsste sie folglich argumentieren, dass sie sich gegenwärtig bereits in einer solchen Krise befindet. Dabei muss sie beachten, dass das Panel bloße politische oder wirtschaftliche Differenzen zwischen den Mitgliedern für sich genommen nicht als ausreichend erachtet hat, um einen Notfall in den internationalen Beziehungen zu begründen.[223] Auch im Rechtsstreit über US-Zölle auf Stahl und Aluminium hatte ein WTO-Panel Ende 2022 ein weiteres Mal über die Voraussetzungen der Sicherheitsausnahme zu entscheiden. US-Präsident Trump hatte sich im Jahr 2018 auf diese Ausnahme berufen, um die von ihm eingeführten zusätzlichen US-Zölle auf Stahl und Aluminium zu rechtfertigen.[224] Das Panel hielt jedoch das Vorliegen eines Notstands nicht für gegeben, da es an einer mit einem Krieg vergleichbaren Auswirkung auf die internationalen Beziehungen fehle.[225] Die USA haben die Entscheidung des Panels nicht anerkannt und Ende Januar 2023 dagegen Berufung eingelegt.[226] Eine Entscheidung eines Berufungsgremiums ist angesichts der derzeitigen Blockade[227] der WTO-Streitschlichtung durch die USA in absehbarer Zeit nicht zu erwarten.

Ob sich die Souveränitätsanforderungen der EU unter Berufung auf eine der Sicherheitsausnahmen rechtfertigen lassen, ist im Ergebnis offen. Es zeichnet sich ab, dass die nationale Sicherheit immer mehr zu einem Vorwand für Schutzmaßnahmen im internationalen Handel werden könnte.[228] Handelsinteressen dürfen jedoch nicht als wesentliche Sicherheitsinteressen „umetikettiert“ werden.[229] Die Sicherheitsausnahmen gelten nur für eine begrenzte Anzahl von Szenarien, von denen die meisten nach Ansicht von Experten nicht auf die gängigen Cybersicherheitsmaßnahmen anwendbar sind. Zudem bestehe Unsicherheit darüber, welche Maßnahmen die Ausnahmen abdecken, um drohenden Cyber- und sonstigen Bedrohungen zu begegnen.[230] Ebenso bleiben Fragen der Beweislast offen. Der Ausgang eines möglichen Streitbeilegungsverfahrens wäre daher ungewiss.[231]

Politische Erwägungen

Ungeachtet des juristischen Ergebnisses einer solchen Abwägung ist ferner unklar, ob es tatsächlich zu einer Beschwerde vor der WTO bzw. zu einer Entscheidung eines WTO-Panels käme, bei der das Panel eine Abwägung zwischen nationalen Sicherheitsbelangen der EU bzw. ihrer Mitgliedstaaten und der angestrebten Handelsliberalisierung vornehmen müsste. Die Ausnahme zur nationalen Sicherheit wurde historisch gesehen eher zurückhaltend angewandt.[232] Die WTO weigerte sich, einen Interessenausgleich zwischen internationalem Handel und nationaler Sicherheit zu schaffen und wich den ihr

[221] Reinsch, W./ Caporal, J. (2019), The WTO’s First Ruling on National Security: What Does It Mean for the United States?, siehe hier.
[222] Reinsch, W./ Caporal, J. (2019), a.a.O.
[223] Reinsch, W./ Caporal, J. (2019), a.a.O.
[224] Reinsch, W./ Caporal, J. (2019), a.a.O.
[225] Siehe Ziffer 7.139 des Panel Reports im WTO Dispute Settlement (DS) 544 vom 9. Dezember 2019, siehe hier.
[226] Siehe hier.
[227] Hoffmann, M. (2024), Blockade der WTO-Streitschlichtung: Wie geht es weiter?, siehe hier; Kessler, D. (2021), Der Konflikt um die WTO-Streitschlichtung, Wissenschaftlicher Dienst des Deutschen Bundestags, siehe hier.
[228] So bereits vermutend Peng, S. (2015), a.a.O., S. 449 (450).
[229] Reinsch, W./ Caporal, J. (2019), a.a.O.
[230] Burri, M. / Kugler, K., a.a.O., S. 422.
[231] Ebenso Propp, K. (2022), European Cybersecurity Regulation Takes a Sovereign Turn, vgl. hier.
[232] Peng, S., Cybersecurity Threats and the WTO National Security Exceptions, Journal of International Economic Law, 2015, A. 449 (459), vgl. hier.

vorgelegten Fragen zur Rechtfertigung aus. Es gibt bislang nur begrenzt einschlägige Rechtsprechung der WTO zu Maßnahmen, die zur Förderung der nationalen Sicherheit ergriffen werden. Zudem ist die Rechtsprechung nicht eindeutig, eröffnet doch die Mehrdeutigkeit der Ausnahmen für die nationale Sicherheit viel juristischen Interpretationsspielraum. Nicht nur war diese Mehrdeutigkeit genau aus diesem Grund verhandlungsgeschichtlich gewollt. Es lässt sich auch mutmaßen, dass WTO-Mitglieder in der Vergangenheit offensichtlich versucht haben, zu vermeiden, dass eine WTO-Entscheidung über Sicherheitsausnahmen zustande kommt. Eher zögerten sie, Fragen, die sie als wichtige Fragen der nationalen Sicherheit ansehen, der WTO vorzulegen. Denn es kann sinnvoll sein, die Auslegung der Sicherheitsausnahmen vage zu lassen, wenn die Mitglieder nicht sicher sind, auf welcher Seite sie in einem Streitfall stehen werden.[233] Die Berufung auf die WTO-Ausnahmen in Handelsstreitigkeiten im Zusammenhang mit Cybersicherheit kann auch deshalb zu unerwünschten Ergebnissen führen, da sich die Gremien mit hochsensiblen Themen befassen müssten.[234] Zwar könnten die Panel-Entscheidungen im Russland-Ukraine-Konflikt sowie im Handelsstreit über die US-Zölle auf Stahl und Aluminium einen Hinweis darauf geben, wie künftige WTO-Panels mit anderen Streitfällen umgehen könnten, bei denen eine Partei sich auf die Sicherheitsausnahme beruft.[235] Unterscheiden sich die Umstände, könnten andere Panels die Frage der nationalen Sicherheit aber auch anders sehen.[236] Insgesamt steht die WTO mit ihren Überlegungen zur Frage der nationalen Sicherheit vermutlich noch immer am Anfang.[237] Bei all dem besteht zudem immer auch die Gefahr, dass Entscheidungen, in denen die Panels die Möglichkeiten der Mitgliedstaaten zu sehr einschränken, die Sicherheitsausnahme in Anspruch zu nehmen, von diesen als inakzeptable Verletzung der nationalen Souveränität gewertet werden und dazu führen, dass sich Mitglieder aus der WTO zurückziehen.

Dass Staaten in Handelskonflikten mit Bezug zur Cybersicherheit auf beiden Seiten stehen können, zeigt auch das Beispiel der USA: zum einen wehrt sich die US-Handelskammer gegen mögliche Souveränitätskriterien der EU im Rahmen der Cybersicherheitszertifizierung mit dem Argument, dass diese die in den USA ansässigen Hyperscaler auf dem europäischen Markt benachteiligen könnten.[238] Auf der anderen Seite möchten die Vereinigten Staaten sich und ihre Bürger selbst schützen, indem sie den Einsatz chinesischer Technologie im Rahmen der Telekommunikation verbieten bzw. mit Handelssanktionen belegen.[239] Umgekehrt hatte China nach den Snowden-Enthüllungen seinen Regulierungsbehörden aufgrund von Cybersicherheitsbedenken verboten, das Microsoft-Betriebssystem Windows 8 auf neuen Computern zu installieren.[240] Die Argumentationsmuster scheinen sich dabei oft zu ähneln: neben einer behaupteten Diskriminierung wird vorgebracht, dass die fragliche Maßnahme den Wettbewerb im betroffenen Sektor ernsthaft beeinträchtigen könne oder werde. Werden die Beschränkungen als Protektionismus empfunden, besteht zudem die Gefahr, dass die betroffenen Staaten mit eigenen Sicherheitsmaßnahmen gegen Technologien oder Dienstleistungen aus dem anderen Staat Vergeltung üben werden.[241] Dieses Risiko darf auch die EU nicht außer Acht lassen. Dennoch ist evident, dass die Problematik – zum eigenen Schutz Ausnahmen von den WTO-Pflichten in Anspruch

[233] Peng, S., Cybersecurity Threats and the WTO National Security Exceptions, a.a.O.
[234] Burri, M. / Kugler, K., a.a.O., S. 422.
[235] Reinsch, W./ Caporal, J. (2019), a.a.O.
[236] Reinsch, W./ Caporal, J. (2019), a.a.O.
[237] Reinsch, W./ Caporal, J. (2019), a.a.O.
[238] Peng, S., a.a.O., S. 449 (455f.).
[239] Siehe etwa Daum, T. (2024), Missing Link: Huawei-Sanktionen – Der Schuss geht nach hinten los, siehe hier.
[240] Peng, S., a.a.O., S. 449 (450).
[241] So etwa die Argumentation der Kritiker eines US-Gesetzes, das die öffentliche Beschaffung chinesischer IT durch ausgewählte US-Bundesbehörden beschränkte, vgl. Peng, S., a.a.O., S. 455f.

nehmen zu wollen, dasselbe aber anderen Staaten nicht zuzugestehen, oder mit den eigenen Maßnahmen Sanktionen anderer Staaten zu provozieren – letztlich mehrere, wenn nicht alle Staaten betrifft.

Betrachtet man die Situation bei Cloud-Diensten, zeigt sich, dass auch andere Staaten eigene Programme zum Schutz sensibler, in der Cloud gespeicherter Daten vorsehen. So haben etwa die USA mit ihrem Federal Risk and Authorization Management Program (FedRAMP)[242] ein regierungsweites Programm eingeführt, das einen standardisierten Ansatz für die Sicherheitsbewertung, -autorisierung und -kontrolle für Cloud-Produkte und Dienste bietet, die von Behörden genutzt werden dürfen. Dieses Programm schreibt auf der höchsten Stufe „High Baseline“ ebenfalls eine Lokalisierung von Daten und Diensten beschränkt auf das US-Territorium oder geografische Standorte mit U.S.-Gerichtsbarkeit vor, um die sensibelsten Daten der US-Regierung in Cloud-Computing-Umgebungen zu schützen.[243] Kritiker des EUCS argumentieren hingegen, die pauschalen Datenlokalisierungs- und Immunitätsvorgaben des EUCS seien nicht mit den flexibleren, risikobasierten und nichtdiskriminierenden System des FedRAMP vergleichbar, das Datenlokalisierungsvorgaben auf bestimmte Systeme in der Hochrisikokategorie begrenze und selbst auf der hohen Kritikalitätsstufe Anbieter zulasse, die nicht in den USA ansässig seien.[244] Laut eines Regelungsvorschlags des US-Verteidigungsministerium denken aber offenbar auch die USA darüber nach, die Bedingungen dahingehend zu ändern, dass Cloud-Dienste mit FedRAMP High alle Regierungsdaten physisch in den Vereinigten Staaten oder deren Randgebieten oder auf Regierungsgelände speichern müssen.[245] Ungeachtet der Unterschiede zwischen den verschiedenen nationalen Programmen zeigt das Beispiel, dass die Gewährleistung der (Cyber-)sicherheit von Cloud-Diensten und sensiblen Daten nicht allein ein europäisches, sondern ein international verbreitetes Bedürfnis ist.

3.6 Zwischenfazit

3.6.1 (Polit-)Ökonomische Perspektive

Die verstärkten Bemühungen der EU, zugleich cybersichere und die digitale Souveränität sicherstellende EU-Märkte für Cloud-Dienste zu etablieren und zu fördern, sind aus geopolitischer und sicherheitspolitischer Perspektive verständlich und nachvollziehbar. Nicht zuletzt die mit dem Wahlsieg Donald Trumps noch weiter gestiegene Unsicherheit der geopolitischen Lage macht deutlich, dass hier zusätzliche Anstrengungen vonnöten sind. Ob jedoch die Etablierung eines europäischen Cybersicherheitszertifizierungsschemas für Cloud-Dienste (EUCS) mit spezifischen „Souveränitätsanforderungen“ in (polit-)ökonomischer Hinsicht ein sinnvoller, geeigneter und zielführender Schritt ist, ist und bleibt umstritten. Letztlich hängt der Erfolg eines jeden EUCS davon ab, ob es als glaubwürdig erachtet wird und, obgleich als freiwilliges Schema konzipiert, in der Praxis auch zur Anwendung kommt. Derzeit stehen sich Befürworter und Gegner von Souveränitätsanforderungen sowohl auf Seiten der politischen Entscheidungsträger als auch auf Seiten der betroffenen Wirtschaftsakteure scheinbar unversöhnlich gegenüber. Dies lässt zumindest zweifeln, dass ein EUCS mit Souveränitätsanforderungen in der Praxis auf breite Akzeptanz stoßen wird. Bevor ein solches EUCS beschlossen wird, gilt es daher, diese Zweifel auszuräumen oder zumindest abzumildern. Ansonsten wird sich das EUCS-Zertifizierungsschema im Wettbewerb mit alternativen Instrumenten wie privaten Gütesiegeln, Labels

[242] https://www.fedramp.gov/.
[243] United States Government (2020), An Update to FedRAMP’s High Baseline SA-9(5) Control, siehe hier.
[244] Propp, K (2023).
[245] Schneider, G./ McGiff, T. (2024), Proposed FAR Rule on Data Localization Would Undermine U.S. Cybersecurity, Competitiveness, siehe hier.

oder Branchenstandards, welche (potenzielle) Cloud-Nutzer über die Cybersicherheitseigenschaften von Cloud-Diensten aufzuklären versprechen, nicht in der Breite durchsetzen. Man könnte argumentieren, dass allen betroffenen Marktakteuren aufgrund der Freiwilligkeit des Schemas die freie Wahl bleibt und es ihnen auch im Falle einer Aufnahme von Souveränitätsanforderungen in das Schema offensteht, Cloud-Dienste zu nutzen, die diese Anforderungen nicht erfüllen. Je eher die EU bzw. die Mitgliedstaaten aber (künftig) geneigt sind, bestimmte Akteure – etwa Betreiber kritischer Infrastrukturen oder Einrichtungen der öffentlichen Verwaltung – dazu zu verpflichten, ausschließlich nach einem EUCS mit strikten Souveränitätsanforderungen zertifizierte Cloud-Dienste zu nutzen, umso wichtiger wird es für die politischen Entscheidungsträger werden, etwaige Zweifel an der Sinnhaftigkeit und Zweckmäßigkeit von Souveränitätsanforderungen zu zerstreuen. Bleiben die angesprochenen Zweifel bestehen, werden diese Akteure entweder zur Verwendung von Cloud-Diensten gedrängt, die nicht oder nur teilweise ihren (Cybersicherheits-)Erwartungen entsprechen, oder sie könnten davon Abstand nehmen, Cloud-Dienste überhaupt zu nutzen. Sofern ein EUCS mit Souveränitätsanforderungen künftig beschlossen werden sollte, das nicht auf breite Akzeptanz stößt, sollte es nicht, auch nicht für einzelne Akteure, zur Pflicht gemacht werden, ausschließlich EUCS-zertifizierte Dienste zu nutzen. In jedem Fall sollten Nutzer alternativ auch konkurrierende Instrumente einsetzen dürfen.

3.6.2 Juristische Perspektive

Souveränitätsanforderungen der dargestellten Art in einem EUCS zu regeln, ist juristisch heikel. Denn es handelt sich nicht lediglich um eine unpolitische Konkretisierung der Regelungen des EU Cybersecurity Act (CSA). Vielmehr sollte die EU strikte Souveränitätsanforderungen, die über die bestehenden Regelungen im Data Act, in der DSGVO und anderen EU-Rechtsakten hinausgehen, gesetzlich (d.h. im Wege einer Verordnung oder einer Richtlinie) und nicht im Rahmen eines EUCS auf der Ebene einer Durchführungsverordnung regeln. Sie sollte für umstrittene Souveränitätsanforderungen wie das Sitzerfordernis, die Datenlokalisierung und die Unternehmenskontrolle bzw. Anforderungen, die die Immunität der Cloud-Anbieter von Drittstaatsrecht sicherstellen sollen, eine gesetzliche Grundlage schaffen. Denn diese Anforderungen können weitreichende Auswirkungen auf den Cloud-Markt in der EU und den internationalen Handel haben, weshalb ihre Etablierung eine wesentliche Grundentscheidung darstellt, die juristisch dem EU-Gesetzgeber vorbehalten ist. Mit Hilfe eines EU-Gesetzes könnten solche Anforderungen demokratisch legitimiert und Grundrechtseingriffe, die mit den Souveränitätsanforderungen einhergehen, bei verhältnismäßiger Ausgestaltung gerechtfertigt werden.

Zur gesetzlichen (Neu-)regelung von Cybersicherheits- und Souveränitätsanforderungen kann sich die EU möglicherweise auf die Kompetenz zur Harmonisierung des Binnenmarkts gemäß Art. 114 AEUV stützen. Je nach Umfang und Ausgestaltung der Regelungen müsste die EU aber ggf. vorrangig die grundfreiheitsspezifische Kompetenznorm zur Harmonisierung des Dienstleistungsverkehrs in Art. 53 Abs. 1 i.V.m. Art. 62 AEUV nutzen, um unterschiedliche mitgliedstaatliche Souveränitätsanforderungen für Cloud-Dienste durch eine EU-Richtlinie zu koordinieren. Weil die EU, wenn sie gesetzgeberisch tätig wird, in die Kompetenz der Mitgliedstaaten eingreift, deren Cybersicherheit und andere Sicherheitsinteressen selbstbestimmt zu regeln, und dies zu einer Absenkung des Schutzniveaus in den Mitgliedstaaten führen kann, muss sie bei der Ausgestaltung der Anforderungen das Subsidiaritäts- und das Verhältnismäßigkeitsprinzip achten. Zwar kann ein hohes EU-weites Cybersicherheitsniveau grundsätzlich am besten auf EU-Ebene erreicht werden. Zum Schutz wichtiger nationaler Interessen wie der öffentlichen Sicherheit, der Landesverteidigung und der öffentlichen Ordnung sollten die Mitgliedstaaten strengere nationale Anforderungen und Zertifizierungsschemata regeln bzw. beibehalten dürfen. Dies gilt umso mehr für Anforderungen, die den Schutz der nationalen Sicherheit der Mitgliedstaaten

sicherstellen sollen. In dem – allerdings eng zu verstehenden – Bereich der nationalen Sicherheit, die die Sicherheit eines Staates im engeren Sinn betrifft, verbleibt die alleinige Regelungskompetenz bei den Mitgliedstaaten, weshalb die EU diesen Bereich aus ihren Regelungen ausklammern muss.

Um Widersprüche und Rechtsunsicherheit zu vermeiden, muss die EU ferner sicherstellen, dass von ihr geregelte Souveränitäts- und sonstige Cybersicherheitsanforderungen mit den Regelungen im Data Act, der DSGVO und anderen Rechtsakten wie der NIS-II-Richtlinie und dem AI Act abgestimmt und angeglichen werden.[246]

Die EU sollte etwaige Souveränitätskriterien so ausgestalten, dass sie nicht erfolgreich vor einem WTO-Panel angefochten werden können, oder sie sollte dieses Risiko zumindest weitestmöglich senken. Dabei sollte die EU darauf achten, die Kriterien so auszugestalten, dass sie nicht als eine offensichtliche oder versteckte protektionistische Handelsregelung missverstanden werden können.

Da auch andere Staaten zunehmend unter Berufung auf die nationale Sicherheit und Souveränität Ausnahmen vom internationalen Freihandel geltend machen und keine Klarheit dahingehend besteht, wie das bestehende internationale Handelsrecht auf digitale Dienstleistungen wie Cloud-Dienste anzubieten ist, müssen sich die EU und ihre Mitgliedstaaten gemeinsam mit ihren Handelspartnern nachdrücklich dafür einsetzen, aktualisierte internationale Regeln für ein modernisiertes, digitales Welthandelsrecht zu vereinbaren. Dabei sollten sie versuchen, auf der Grundlage von Gegenseitigkeit und Gleichheit maßgeschneiderte Ausnahmen für die Daten- und Cybersicherheit und die „nationale Souveränität“ auf internationaler Ebene zu etablieren, oder einen anderweitigen Konsens zu finden. In diesem Zusammenhang sollte u.a. auch geklärt werden, ob Ausnahmen vom Freihandel künftig nicht nur zum Schutz personenbezogener Daten, sondern auch zum Schutz der Cybersicherheit sowie zum Schutz von Geschäftsgeheimnissen und sensiblem Know-How implementiert werden sollten. In bilateraler Hinsicht sollte auch (weiterhin) der Rat für Handel und Technologie (Trade and Technology Council) als Forum für eine Diskussion über die gegenseitigen Ansätze zur Bereitstellung von Cloud-Diensten in der Privatwirtschaft und an die öffentliche Hand genutzt werden.[247] Es gilt, in dem immer komplexer werdenden Spannungsfeld zwischen internationalem Freihandel und staatlichen Sicherheitsinteressen[248] ein konsensfähiges Gleichgewicht zu finden, um die Herausforderungen der datengesteuerten Wirtschaft zu meistern.

3.6.3 Was folgt aus dieser Analyse?

Aus der obigen Analyse folgt: Sowohl die umstrittene Sinnhaftigkeit und Zweckmäßigkeit der diskutierten Souveränitätsanforderungen (innerhalb eines EUCS) und das Risiko der fehlenden Akzeptanz eines EUCS, das solche Anforderungen enthält, als auch mögliche juristische Fallstricke der zwischenzeitlich angedachten Lösung, Souveränitätsanforderungen im Rahmen eines EUCS zu regeln und dieses perspektivisch für bestimmte Akteure verpflichtend zu machen, sprechen dafür, dass es eines neuen Anlaufs bedarf, um (Aus-)Wege aus der festgefahrenen Debatte zu finden. Im folgenden Kapitel sollen einige mögliche (Aus-)Wege skizziert werden.

[246] Stellungnahme der Niederlande zum Non-paper von DE, ES, FR und IT zu den EUCS-Anforderungen an die Immunität gegenüber Nicht-EU-Gesetzen (2021), vgl. hier.
[247] Propp, K. (2022), European Cybersecurity Regulation Takes a Sovereign Turn, 12. September 2022, abrufbar hier.
[248] Peng, S. (2015), a.a.O., S. 449 (450).

4 (Aus-)Wege aus dem Zertifizierungsdilemma

Auch nach jahrelangen Diskussionen konnten sich die EU-Kommission, der EU-Gesetzgeber, die ENISA und andere an der Entwicklung eines EUCS beteiligte Gremien und Stakeholder nicht auf eine finale Version eines EUCS – ob mit oder ohne Souveränitätsanforderungen – einigen, und ein Kompromiss, der alle Seiten zufriedenstellt, scheint derzeit nicht absehbar. Es ist daher an der Zeit, über alternative Ansätze nachzudenken. Im Folgenden sollen, Schritt für Schritt, mögliche Auswege aus der entstandenen Sackgasse beschrieben und diskutiert werden. Dabei werden auch die Ideen mit einbezogen, die Mario Draghi in seinem Bericht zur Stärkung der Wettbewerbsfähigkeit[249] und die Kommission in ihrem „Mission Letter" an Henna Virkkunen[250], die neue Vizepräsidentin für „Technologische Souveränität, Sicherheit und Demokratie", präsentiert haben.[251]

4.1 Beschluss des EUCS ohne Souveränitätsanforderungen

Die EU-Kommission sollte das EUCS, ungeachtet der anhaltenden Diskussionen über die Souveränitätsanforderungen, nun zügig beschließen. Eine weitere Verzögerung wäre nicht sachdienlich. Auch wenn das EUCS kein „Allheilmittel" darstellt und nicht allen Gründen für Marktversagen in den Märkten für (cybersichere) Cloud-Dienste vollumfänglich begegnet (siehe Kapitel 2.3), kann es über den Abbau von Informationsasymmetrien den Markt für cybersichere Cloud-Dienste beleben und das Vertrauen potenzieller Nutzer in die Dienste stärken. Allein dies wäre ein Beitrag zur Stärkung der Cybersicherheit von Cloud-Lösungen. Ferner würde damit Rechts- und Planungssicherheit für die betroffenen Akteure geschaffen und für den Binnenmarkt eine einheitliche Lösung etabliert. Auf Souveränitätsanforderungen für Cloud-Dienste sollte aufgrund rechtlicher Bedenken (siehe Kapitel 3.5 und cep**Analyse**), aber auch aufgrund der derzeit bestehenden politischen Uneinigkeit und der Gefahr fehlender Akzeptanz eines EUCS mit solchen Anforderungen zunächst verzichtet werden. Über solche Anforderungen sollte vielmehr auf politischer Ebene – also durch das Europäische Parlament und den Rat – entschieden werden und nicht im Rahmen der Festlegung technischer Vorgaben im Rahmen eines Durchführungsrechtsakts.

4.2 Überarbeitung des EU-Rechtsakts zur Cybersicherheit (CSA)

Bereits im Frühjahr 2019 ist der EU-Rechtsakt zur Cybersicherheit (CSA, s. cep**Analyse**) in Kraft getreten und mit ihm wurde ein Rahmen für die Zertifizierung der Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen auf EU-Ebene etabliert. Es hat sich gezeigt, dass sich dieser Cybersicherheitszertifizierungsrahmen in der Praxis jedoch nicht als hinreichend effizient erwiesen hat und es sind immer wieder Verzögerungen bei der Annahme von EU-Zertifizierungsschemata entstanden. Der CSA sieht vor,

[249] EU-Kommission (2024a).

[250] EU-Kommission (2024b), Mission Letter by Ursula von der Leyen, President of the European Commission for Henna Virkunnen, Executive Vice-President-designate for Tech Sovereignty, Security and Democracy, 17. September 2024.

[251] In ihren Antworten auf spezifische Fragen der Abgeordneten des Europäischen Parlaments im Vorfeld ihrer Anhörung am 12. November 2024 im Europäischen Parlament äußerte sich Henna Virkunnen zur Zukunft eines EUCS wie folgt „*Ich begrüße das freiwillige EU-Zertifizierungssystem für Cybersicherheit für Cloud-Dienste (EUCS), da es die Transparenz über das Sicherheitsniveau von Cloud-Diensten erhöhen wird. Sobald es eingeführt ist, wird es die derzeitige Fragmentierung bei der Zertifizierung beheben und die finanziellen Hürden für Anbieter senken, die sichere Cloud-Lösungen in der EU anbieten wollen. Gleichzeitig bin ich mir neben den technischen Anforderungen auch der sicherheitspolitischen Herausforderungen bewusst, die sich im aktuellen geopolitischen Kontext stellen. Auf diese Herausforderungen werde ich bei der Arbeit an den verschiedenen Cloud-Initiativen in meiner Amtszeit achten" (übersetzt via deepl.com)* [Europäisches Parlament (2024), Questionnaire to the Commissioner-designate, Henna Virkunnen, Executive Vice-President for Tech Sovereignty, Security and Democracy].

dass die Kommission bis Ende Juni 2024 eine Bewertung der „Wirkung, Wirksamkeit und Effizienz“ der Vorschriften zur Cybersicherheitszertifizierung vorzunehmen hatte.[252] Die Schlussfolgerungen dieser Bewertung muss sie unter anderem dem Europäischen Parlament und dem Rat vorlegen.[253] Auch wenn die Kommission ihre Schlussfolgerungen noch nicht veröffentlicht hat, hat sie bereits im Februar 2024 im Rahmen eines Konsultationsverfahrens mit der Evaluierung des Rechtsakts begonnen.[254] Ferner erhielt Henna Virkkunen, die neue EU-Vizepräsidentin für „Technologische Souveränität, Sicherheit und Demokratie“, in ihrem „Mission Letter“ den Auftrag, in der nun begonnenen Legislaturperiode den Prozess der Annahme von europäischen Cybersicherheitszertifizierungsschemata zu verbessern, um die Cybersicherheit zu stärken[255]:

“You will contribute to strengthening cybersecurity to protect our industries, citizens and public administrations against internal and external threats, ***notably by improving the adoption process of European cybersecurity certification schemes****.”*[256]

Die anstehende Überarbeitung des CSA böte jedenfalls eine gute Gelegenheit, die Vorgaben zur Cybersicherheitszertifizierung zu überarbeiten. Bei dieser Überarbeitung wären insbesondere die folgenden Anpassungen sinnvoll:

- Klare Fokussierung auf die Stärkung der Cybersicherheit: Die Stärkung der Cybersicherheit sollte bei der Ausgestaltung von Zertifizierungsschemata immer im Vordergrund stehen. Sofern mit einem Schema zusätzliche Ziele – z.B. industrie- oder geopolitische Ziele – verfolgt werden, sollte die Verfolgung dieser Ziele dem primären Ziel in jedem Fall nicht entgegenstehen.[257] Auch sollte die ENISA diese weiteren Ziele bei einem Schema nur dann berücksichtigen dürfen, wenn sie hierfür das Mandat der Gesetzgeber erhalten hat. Dies bedeutet, dass diese Ziele bereits auf Level 1 im CSA verankert werden sollten. Der Spielraum der ENISA bzw. der Kommission, auf Level 2 zu agieren, d.h. im Rahmen der Formulierung eines Durchführungs- oder delegierten Rechtsakts, sollte hier eng begrenzt sein. Sollten den Gesetzgebern diese ergänzenden Ziele wichtig sein, ist auch darüber nachzudenken, diese zu hierarchisieren sowie Leitplanken dafür zu etablieren, wie die ENISA bzw. die Kommission im Falle von etwaigen Zielkonflikten vorzugehen haben. Schließlich bedarf es klarer Kriterien, welche Aspekte die ENISA bei der Ausgestaltung eines Schemas berücksichtigen und welchen sie keine Bedeutung beimessen dürfen soll.
- Klare Fristen für die Entwicklung eines Cybersicherheitszertifizierungsschemas: Der CSA setzt den an der Ausarbeitung eines Cybersicherheitszertifizierungsschemas beteiligten Akteuren derzeit keine Fristen, wie lange ein solcher Ausarbeitungsprozess dauern darf. Zwischen der

[252] Art. 67 Abs. 1 bis 3 Verordnung (EU) 2019/881.
[253] Art. 67 Abs. 4 Verordnung (EU) 2019/881.
[254] EU-Kommission (2024c), Konsultation, Bewertung des Rechtsakts zur Cybersicherheit, 13. Februar – 5. März 2024, s. hier.
[255] EU-Kommission (2024b).
[256] Der Rat rief am 6. Dezember 2024 zu weiteren Verbesserungen und Maßnahmen im Hinblick auf die Entwicklung von EU-Schemata zur Zertifizierung der Cybersicherheit auf. In Schlussfolgerungen zur ENISA „betont“ er, dass die Mitgliedstaaten und die Industrie hinsichtlich der langwierigen Prozesse zur Ausarbeitung von Zertifizierungsschemata „besorgt“ seien. Er „fordert“ „nachdrücklich“ schlankere, transparentere und schnellere Ansätze zur Entwicklung solcher Schemata. Dies soll bei der geplanten Überarbeitung der CSA berücksichtigt werden. Zudem „erinnert“ er die ENISA und die Kommission daran, alle einschlägigen Akteure „rechtzeitig“ zu konsultieren [Rat (2024), Schlussfolgerungen zur ENISA, Rat „Verkehr, Telekommunikation und Energie“, Telekommunikation, 6. Dezember 2024, abrufbar hier].
[257] Hierbei könnte man sich an einem Ansatz orientieren, der sich in der EU-Verordnung zur Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen („grüne Taxonomie“) wiederfindet. Danach muss ein Schema einen „wesentlichen Beitrag zur Verwirklichung des Ziel der Stärkung der Cybersicherheit leisten. Werden andere Ziele – zusätzlich – verfolgt, darf dies nicht zu einer „erheblichen Beeinträchtigung“ bei der Erreichung des Cybersicherheitsziel führen („do not significantly harm, DNSH-Konzept“) [ähnlich siehe Art. 3 der Verordnung (EU) 2020/852 über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen und zur Änderung der Verordnung (EU) 2019/2088].

Auftragserteilung an die ENISA durch die Kommission und der Verabschiedung eines neuen Schemas kann daher viel Zeit verstreichen, ohne dass es ein Ergebnis gibt (vgl. den noch immer nicht abgeschlossenen Prozess zur Erarbeitung eines EUCS). Das Fehlen solcher Fristen und die damit einhergehenden Verzögerungen bei der Etablierung neuer Schemata schwächt jedoch nicht nur die Glaubwürdigkeit der Zertifizierung der Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen an sich, sondern sorgt auch für einen Mangel an Rechts- und Planungssicherheit für Cloud-Anbieter und -Nutzer. Bei der Überarbeitung des CSA sollten daher klare Fristen für die Etablierung neuer Schemata – beispielsweise maximal zwei Jahre – verankert werden. Auch könnte die Länge von Verfahren zur Konsultation der verschiedenen Interessenträger bereits auf Level 1 vorgegeben werden, um den Pfad zur Erarbeitung eines Schemas noch genauer vorzuzeichnen und zu strukturieren.

- Pflicht zur Transparenz in Bezug auf den aktuellen Sachstand bei einem Schema: In den vergangenen Jahren hat sich gezeigt, dass es für Interessenträger, aber auch für die breite Öffentlichkeit nur sehr schwer möglich war, sich über den aktuellen Sachstand bei einzelnen Schemata zu informieren. Neue, angepasste und überarbeitete Fassungen der Entwürfe einzelner Schemata gelangten oft, wenn überhaupt, nur über spezialisierte Medien an die Öffentlichkeit, während sie durch die ENISA selbst nur sporadisch proaktiv veröffentlicht wurden. Hier erscheint dringend ein Mehr an Transparenz vonnöten, um das Vertrauen in neue Schemata zu gewährleisten. Diese Transparenz sollte es interessierten Parteien ermöglichen, neue oder angepasste Anforderungen zu kommentieren und zu hinterfragen; insbesondere auch solche Vorgaben, die als nichttechnisch angesehen werden. Die zusätzliche Transparenz sollte in jedem Fall über den bereits jetzt im CSA vorgeschriebenen Konsultationsprozess durch die ENISA hinausgehen.[258] Die neuen Transparenzvorgaben, die im Rahmen der Änderungsverordnung in Bezug auf verwaltete Sicherheitsdienste eingeführt wurden, sind hier ein guter erster, aber noch nicht ausreichender Schritt.[259,260]
- Delegierter Rechtsakt statt Durchführungsrechtsakt: Die Kommission sollte künftige EU-Zertifizierungsschemata (d.h. auch ein künftiges EUCS) mittels delegierten Rechtsakten (Art. 290 AEUV) statt mittels Durchführungsrechtsakten (Art. 291 AEUV) festlegen. Dies würde auch dessen demokratische Legitimation stärken. Gleichzeitig sollte der EU-Gesetzgeber alle wesentlichen Aspekte selbst auf Level 1 regeln, d.h. all jene Vorgaben, durch die die grundsätzliche Ausrichtung der EU-Politik umgesetzt wird[261], also etwa auch, ob – und wenn ja welche – Souveränitätsanforderungen bei der Ausgestaltung eines EUCS auf Level 2 zu berücksichtigen sind.
- Vertrauen potenzieller Verwender zertifizierter IKT-Produkte, -Dienste oder -Prozesse in neue EU-Schemata prüfen: Ein zentrales und wichtiges Ziel des EU-Rahmens zur Cybersicherheitszertifizierung ist es, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse stärken.[262] Das Vertrauen kann

[258] Die ENISA muss bei der Ausarbeitung eines möglichen Schemas alle in Frage kommenden Interessenträger im Wege eines „förmlichen, offenen, transparenten und inklusiven Konsultationsprozesses“ konsultieren [s. Art. 49 Abs. 3 Verordnung (EU) 2019/881.

[259] Verordnung (EU) 2024/… des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) 2019/881 in Bezug auf verwaltete Sicherheitsdienste (vom Rat final beschlossen am 2. Dezember 2024, siehe hier).

[260] Die Kommission muss künftig öffentlich darüber informieren, wenn sie die ENISA ersucht, ein Schema zur Zertifizierung der Cybersicherheit auszuarbeiten oder ein bestehendes Schema zu überprüfen. Das Europäische Parlament und der Rat können die Kommission und die ENISA während der Ausarbeitung eines Schemas dazu auffordern, vierteljährlich über den Entwurf eines Schemas Informationen bereitzustellen. Die ENISA kann dem Europäischen Parlament und dem Rat, sofern Einvernehmen mit der Kommission besteht, relevante Teile eines Entwurfs eines Schemas mit der erforderlichen Vertraulichkeit und gegebenenfalls in eingeschränkter Form zugänglich machen [neuer Art. 49a Verordnung (EU) 2024/…].

[261] EuGH, Urteil vom 27. Oktober 1992, Rs. C-240/90, Deutschland./.Kommission, ECLI:EU:C:1992:408, Rn. 37. Vgl. dazu bereits oben Kapitel 3.5.1.

[262] Erwägungsgründe 65 und 69 Verordnung (EU) 2019/881.

jedoch nur dann gesteigert werden, wenn ausgearbeitete EU-Schemata zur Zertifizierung der Cybersicherheit und die auf diesen beruhende Zertifikate als glaubwürdig erachtet bzw. auf Seiten der potenziellen Nutzer als vertrauensfördernd wahrgenommen werden. Ist dies nicht der Fall, sind sie letztlich wertlos. Daher erscheint es sinnvoll, vor dem Erlass eines neuen Schemas die potenziellen Nutzer der nach dem Schema zu zertifizierenden IKT-Produkte, -Dienste oder -Prozesse spezifisch dazu zu konsultieren. Dabei sollten sowohl Nutzer befragt werden, denen es freisteht, die zertifizierten Produkte, Dienste oder Prozesse zu nutzen, als auch Nutzer, die (ggf. künftig) dazu verpflichtet sind bzw. verpflichtet werden sollen. Bei der Einholung von Meinungen zu einem ausgearbeiteten Schema sollten die Fragen im Vordergrund stehen, ob ein Schema das Vertrauen fördert, ob es tatsächlich für zielführend, zweckmäßig und notwendig gehalten wird und ob es letztlich auf eine breite Akzeptanz stößt.

- Frühzeitige Einbindung der EU-Gesetzgeber: Mit der in Punkt 1 propagierten Umstellung von Durchführungsrechtsakten auf delegierte Rechtsakte geht bereits eine Stärkung der demokratischen Legitimation einher. Um politischen Konflikten über die Ausgestaltung von Cybersicherheitszertifizierungsschemata jedoch noch zusätzlich vorzubeugen, erscheint es geboten, die politischen Entscheidungsträger schon frühzeitig in die Erarbeitung der Schemata einzubinden, ihnen jedoch auch klare Grenzen der „Einmischung“ in den primär technischen Ausgestaltungsprozess vorzugeben.
- Grundsätzliche Beibehaltung des freiwilligen Ansatzes: Nach dem CSA ist der Rückgriff auf eine europäische Cybersicherheitszertifizierung in der Regel freiwillig.[263] An diesem Grundsatz sollte auch im Rahmen der Überarbeitung des Rechtsakts festgehalten werden, um keine übermäßigen neuen Markteintrittsbarrieren zu schaffen oder Innovationen auszubremsen. Auch ohne verpflichtende EU-Zertifizierung haben beide Marktseiten – Cloud-Anbieter und Cloud-Nutzer – die Möglichkeit, sich für oder gegen die Verwendung eines EU-Zertifikats zu entscheiden. Ist ein Zertifikat ein wichtiges Qualitätsmerkmal für potenzielle Cloud-Nutzer, wird es sich am Markt auch durchsetzen und Cloud-Anbieter werden entsprechend reagieren (müssen), um am Markt zu bestehen – und umgekehrt.
- Zentrale Eckpfeiler für Cloud-Cybersicherheitszertifizierungsschemata: Die in einem Cloud-Cybersicherheitszertifizierungsschema festgelegten Anforderungen sollten risikobasiert und faktenorientiert sein. Sie sollten das Ergebnis einer objektiven Risikobewertung widerspiegeln, welche die Wahrscheinlichkeit und die Folgen unerwünschter potenzieller Cybersicherheitsvorfälle berücksichtigt. Ferner müssen die Anforderungen die Verhältnismäßigkeit wahren. Denn jede regulatorische Vorgabe zur Nutzung von – nur bestimmten – Cloud-Diensten stellen eine Einschränkung der unternehmerischen Freiheit dar und bedürfen somit einer Rechtfertigung. In jedem Fall muss der Zusatznutzen, der durch den Rückgriff auf ein Zertifikat generiert wird bzw. werden soll, in einem angemessenen Verhältnis zu den (voraussichtlichen) verursachten Zusatzkosten stehen. Auch sollte ein Cloud-Schema prinzipiell möglichst wettbewerbsneutral ausgestaltet sein. Jede regulatorische Anforderung an (noch) zulässige Cloud-Dienste sollte keinen Anbieter per se bevorzugen, benachteiligen oder gar gänzlich ex ante ausschließen. Jeder Cloud-Anbieter sollte grundsätzlich die Möglichkeit haben, Zertifizierungen egal welcher Vertrauenswürdigkeitsstufe für seine angebotenen Cloud-Dienste erlangen zu dürfen.

[263] Erwägungsgrund 91 und Art. 56 Abs. 2 Verordnung (EU) 2019/881.

4.3 Überarbeitung der NIS-2-Richtlinie

Die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union [Richtlinie (EU) 2022/2555, NIS-2-Richtlinie] gilt als die erste horizontale Rechtsvorschrift auf EU-Ebene zur Cybersicherheit. Sie wird derzeit von den Mitgliedstaaten – vielfach nicht fristgerecht[264] – in nationales Recht umgesetzt. Die Richtlinie verlangt von den Mitgliedstaaten sicherzustellen, dass insbesondere die inländischen „wesentlichen" und „wichtigen" Einrichtungen „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen" ergreifen müssen, die sie in die Lage versetzen, die Risiken für die Sicherheit ihrer Netz- und Informationssysteme beherrschen zu können. Die Maßnahmen sollen ferner „die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste verhindern oder möglichst gering halten".[265] Die Maßnahmen sollen auch Schritte zur Wahrung der „Sicherheit der Lieferkette" und mithin auch „sicherheitsbezogene" Aspekte im Hinblick auf die Beziehungen zwischen einer Einrichtung und ihren unmittelbaren Anbietern oder Diensteanbietern umfassen. Dabei müssen die Einrichtungen auch die Schwachstellen dieser Anbieter und deren Cybersicherheitspraxis in den Blick nehmen.[266,267]

Die NIS-2-Richtlinie beschränkt die Auswahl von Anbietern oder Diensteanbietern derzeit nicht a priori. Wesentlichen und wichtigen Einrichtungen steht es damit grundsätzlich offen zu entscheiden, ob und wenn ja welche Cloud-Dienste sie – im Rahmen der Risikomanagementmaßnahmen, die sie zu verfolgen haben – nutzen wollen. Die Mitgliedstaaten haben jedoch die Möglichkeit, sie dazu zu verpflichten, nur spezielle IKT-Produkte, -Dienste – einschließlich Cloud-Dienste – oder -Prozesse nutzen zu dürfen, die nach einem EU-Schema zur Zertifizierung der Cybersicherheit zertifiziert sind. Nur ein solches Zertifikat würde dann den Nachweis erbringen, dass die Einrichtung den vorgeschriebenen Risikomanagementmaßnahmen Rechnung trägt.[268]

Diese beschriebene regulatorische Herangehensweise weist jedoch einige Schwächen auf, die im Rahmen einer Überarbeitung der NIS-2-Richtlinie angegangen werden sollten:

1. Einheitlichere Identifizierung von wesentlichen und wichtigen privaten Einrichtungen

Zunächst sollten die Kriterien und Vorgehensweisen zur Identifizierung wesentlicher und wichtiger Einrichtungen durch die Mitgliedstaaten überarbeitet werden. Zwar ist es mit der Überarbeitung der NIS-2-Richtlinie im Jahr 2022 gelungen, diesbezüglich den Spielraum der Mitgliedstaaten und damit Regulierungsarbitrage und Wettbewerbsverzerrungen einzugrenzen. Jedoch sollte bei der Identifizierung nicht nur auf die Größe der Einrichtung abgestellt werden – dies ist derzeit das zentrale Kriterium – sondern auch auf andere Faktoren, wie etwa die Anzahl der Kunden bzw. Nutzer einer Einrichtung

[264] Am 28. 11. 2024 hat die EU-Kommission beschlossen, Vertragsverletzungsverfahren gegen insgesamt 23 Mitgliedstaaten (u.a. Deutschland, Spanien, Frankreich, die Niederlande, Österreich und Polen) einzuleiten, Diese Länder haben bis zu diesem Datum die NIS-2-Richtlinie nicht vollständig umgesetzt (s. hier).

[265] Art. 21 Abs. 1, Richtlinie (EU) 2022/2555.

[266] Art. 21 Abs. 2 und 3, Richtlinie (EU) 2022/2555.

[267] Dies umfasst insbesondere die Festlegung eines „Konzepts für die Sicherheit der Lieferkette". Dieses muss „Kriterien für die Auswahl von Anbietern und Diensteanbietern und die Auftragsvergabe an sie" enthalten, und zwar u.a. zu deren Cybersicherheitsverfahren, deren Fähigkeit von der betreffenden Einrichtung festgelegte Cybersicherheitsspezifikationen zu erfüllen, zur allgemeinen Qualität und Resilienz der IKT-Produkte und -Dienste sowie zur Fähigkeit der Einrichtung, ihre Versorgungsquellen zu diversifizieren und Abhängigkeiten von bestimmten Anbietern zu begrenzen. Ferner müssen Verträge mit Anbietern und Diensteanbietern – soweit angemessen – Cybersicherheitsanforderungen in Form von Leistungsvereinbarungen enthalten. Auch müssen bspw. Sicherheitsanforderungen festgelegt werden, die für die zu erwerbenden IKT-Dienste oder IKT-Produkte gelten müssen und die von den Anbietern zugesichert werden müssen [siehe Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. Oktober 2024 mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 […]].

[268] Art. 24, Richtlinie (EU) 2022/2555.

abgestellt werden. Die unmittelbare Größe einer Einrichtung deutet nicht zwangsläufig und alleinig auf ein höheres Cybersicherheitsrisiko hin. Auch sollte der Anwendungsbereich der NIS-2-Richtlinie immer nur auf jene Einrichtungen abstellen, die für das Funktionieren einer Gesellschaft zentral sind. In jedem Fall sollte die Festlegung derjenigen Einrichtungen, die in den Anwendungsbereich der Richtlinie fallen sollen, möglichst einheitlich erfolgen, um zu verhindern, dass sich einzelne relevante Akteure in den Mitgliedstaaten den Sicherheitsanforderungen der Richtlinie entziehen oder es zu Wettbewerbsverzerrungen kommt. Eine solche einheitliche Festlegung wäre insbesondere für jene Unternehmen bzw. Sektoren von Bedeutung, die in grenzüberschreitender Konkurrenz zueinanderstehen (z. B. Banken, Energieunternehmen, Firmen im Verkehrssektor). Eine möglichst einheitliche Vorgehensweise würde sicherstellen, dass für alle Einrichtungen, die vergleichbaren Cybersicherheitsrisiken unterliegen, auch dieselben Vorgaben gelten, insbesondere auch im Hinblick auf Anforderungen zur (Aus-)Wahl geeigneter Cloud-Dienste.

2. Prüfung einer Pflicht für bestimmte wesentliche und wichtige Einrichtungen zur ausschließlichen Nutzung zertifizierter Cloud-Dienste

Sodann ist zu prüfen, ob einzelne, unter den Anwendungsbereich der NIS-2-Richtlinie fallende (Gruppen von) nicht-staatlichen Einrichtungen explizit verpflichtet werden sollten, nur noch Cloud-Dienste einsetzen zu dürfen, die nach einem künftigen EUCS zertifiziert sind.[269] Zwar erlaubt die Richtlinie den Mitgliedstaaten bereits heute, eine solche Pflicht zu verankern. Diese Öffnungsklausel birgt jedoch die Gefahr unterschiedlichster Vorgehensweisen, einer regulatorischen Zersplitterung und damit einer Schwächung des digitalen Binnenmarkts. Deshalb erscheint es grundsätzlich sinnvoll, eine derartige Pflicht nur für solche private Einrichtungen in den Blick zu nehmen, die in hochsensiblen Tätigkeitsfeldern aktiv sind, wobei die Entscheidung darüber, welche dies sind, in erster Linie eine (gesellschafts-)politische Frage ist. Ferner sollte eine solche Pflicht nur für diejenigen nicht-staatlichen Einrichtungen gelten, bei denen davon ausgegangen werden kann, dass größere Cybersicherheitsrisiken für Dritte entstehen könnten, wenn die Einrichtungen selbst keine Cloud-Dienste auf einem hohen Sicherheitsniveau einsetzen würden, d.h. in Fällen, bei denen Einrichtungen potentielle Schäden bei Dritten bei der Wahl des Cloud-Dienstes nicht in ihr Entscheidungskalkül mit einbeziehen (mangelnde Internalisierung negativer externer Effekte). Außerdem könnte eine solche Pflicht insbesondere dann sinnvoll sein, wenn die entsprechenden Einrichtungen nicht ausschließlich national, sondern auch grenzüberschreitend tätig sind oder sein könnten (s. oben).

3. Zersplitterung beim Anwendungsbereich im Hinblick auf öffentliche Verwaltungen reduzieren und Prüfung einer Pflicht zur Nutzung von zertifizierten Cloud-Diensten für ausgewählte Einrichtungen der öffentlichen Verwaltung

Die EU sollte auch die Einführung einer Pflicht zur ausschließlichen Nutzung zertifizierter Cloud-Dienste für bestimmte und eng definierte öffentliche Einrichtungen prüfen, sofern diese besonders sensible Daten in der Cloud verarbeiten und speichern wollen.[270] In diesem Zusammenhang wäre es zunächst sinnvoll, den Anwendungsbereich der NIS-2-Richtlinie auch im Hinblick auf Einrichtungen der öffentlichen Verwaltung zu überarbeiten und stärker zu harmonisieren. Derzeit fallen Einrichtungen der öffentlichen Verwaltung in den Geltungsbereich, wenn es sich bei ihnen – unabhängig von ihrer Größe –

[269] Dies setzt natürlich die vorherige Annahme des EUCS voraus und sollte zudem nicht so verstanden werden, dass die betroffenen Einrichtungen überhaupt Cloud-Dienste einsetzen müssen.

[270] Die betreffenden öffentlichen Einrichtungen sollten gleichwohl immer die Option haben gänzlich auf Cloud-Dienste zu verzichten.

um Einrichtungen der öffentlichen Verwaltung auf Ebene der der Zentralverwaltung[271] oder um Einrichtungen auf regionaler Ebene handelt; letztere jedoch nur, wenn sie Dienste erbringen, „deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte“[272].

Dagegen haben die Mitgliedstaaten ein Wahlrecht, die NIS-2-Richtlinie auch auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene anzuwenden.[273] Erbringt eine Einrichtung der öffentlichen Verwaltung Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, ist sie ganz generell vom Anwendungsbereich ausgenommen.[274]

Der daraus resultierende „Flickenteppich“ hinsichtlich der Anwendbarkeit der NIS-2-Richtlinie auf öffentliche Einrichtungen sollte überwunden bzw. weiter eingegrenzt werden. Für die Aufnahme in den Geltungsbereich sollte beispielsweise nicht primär die Ebene – zentral, regional oder lokal – entscheidend sein, sondern vielmehr und vordergründig, welche gesellschaftlichen und volkswirtschaftlichen Auswirkungen der Ausfall bzw. die Kompromittierung der entsprechenden öffentlichen Verwaltung für den betreffenden EU-Mitgliedstaat, aber auch EU-weit hätte.[275] Auch sollte eine wichtige Rolle spielen, inwiefern eine öffentliche Verwaltung bzw. eine bestimmte Kategorie von öffentlicher Verwaltung eine Binnenmarktrelevanz aufweist, d.h. inwiefern sie beispielsweise im Rahmen ihrer Tätigkeiten Daten und Informationen mit Verwaltungen in anderen EU Mitgliedstaaten teilt bzw. austauscht. Würde man diesen Flickenteppich stopfen, einheitliche Kriterien für die (Nicht-)Aufnahme öffentlicher Verwaltungen definieren und insbesondere auch Verwaltungen unterhalb der Ebene der Zentralregierung stärker in den Fokus nehmen, wäre bereits einiges zur Stärkung der Cybersicherheit in der EU erreicht.

Die Vereinheitlichung des Anwendungsbereichs der NIS 2-Richtlinie in Bezug auf Einrichtungen der öffentlichen Verwaltung könnte sodann die Grundlage dafür bilden, a priori genauer festzulegen, dass bestimmte Verwaltungen, die dann der NIS 2-Richtlinie unterliegen würden, künftig nur noch Cloud-Dienste nutzen dürfen, die nach einem EU-Schema zur Zertifizierung der Cybersicherheit zertifiziert sind.[276] Für diese Schritte wäre über eine Anpassung des Artikels 24 der NIS-2-Richtlinie nachzudenken.[277] Dabei könnte die Option für die Mitgliedstaaten, Einrichtungen zur Nutzung von nach EU-Cybersicherheitszertifizierungsschema zertifizierten Cloud-Diensten verpflichten zu „können“, für weniger kritische Umgebungen aufrechterhalten werden. Gleichzeitig wäre zu überlegen, für öffentliche Einrichtungen, die (hoch-)sensible Daten verwalten, verarbeiten und speichern, oder bei denen ein regelmäßiger (grenzüberschreitender) Austausch mit anderen öffentlichen Einrichtungen stattfindet (d.h. insbesondere Verwaltungen mit Relevanz für den gemeinsamen Binnenmarkt), aus der Option

[271] Art. 2 Abs. 2 lit. f lit. i NIS-2-Richtlinie.
[272] Art. 2 Abs. 2 lit. f lit. ii NIS-2-Richtlinie.
[273] Art. 2 Abs. 5 lit. a NIS-2-Richtlinie.
[274] Art. 2 Abs. 7 NIS-2-Richtlinie.
[275] Die bestehende Ausnahmeregelung für Einrichtungen der öffentlichen Verwaltung, die Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, sollte jedoch aufrechterhalten werden. Eine Mitberücksichtigung dieser Einrichtungen würde wohl zu sehr in die Hoheitsrechte der einzelnen Mitgliedstaaten hineinragen.
[276] Dies sollte nicht dergestalt verstanden werden, dass Einrichtungen der öffentlichen Verwaltung ganz generell auf Cloud-Dienste einsetzen müssen. Sie sollten auch künftig gänzlich auf der Einsatz verzichten dürfen.
[277] Artikel 24 sieht insbesondere vor, dass „die Mitgliedstaaten […] wesentliche und wichtige Einrichtungen dazu verpflichten [können], spezielle IKT-Produkte, -Dienste und -Prozesse zu verwenden, die von der wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft werden und die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung, die gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifiziert sind […].

(„können“) eine Pflicht („müssen“) zu machen.[278] Im Rahmen einer Änderung des Artikel 24 könnten sodann zugleich die Vertrauenswürdigkeitsstufen vorgegeben werden, die den verpflichteten öffentlichen Einrichtungen dann künftig noch offenstehen. Dies könnte der Entwicklung cybersicherer Märkte für Cloud-Dienste in der EU Auftrieb verschaffen, Größenvorteile auf Seiten interessierter Cloud-Dienste-Anbieter ermöglichen und mithin auch einen Beitrag zur Reduktion der Kosten der Nutzung sicherer Cloud-Dienste leisten. Der hier skizzierte Ansatz könnte daher eine mögliche erste Blaupause für Henna Virkkunen sein, den in ihrem sogenannten „Mission Letter“ skizzierten Vorschlag für die Schaffung einer „EU-weiten Cloud Politik für öffentliche Einrichtungen“ umzusetzen.[279]

4. Eingrenzung des Spielraums der EU-Kommission, Einrichtungen zur Nutzung zertifizierter Cloud-Dienste zu verpflichten

Derzeit kann die Kommission nach der NIS-2-Richtlinie auch mittels delegierter Rechtsakte „Kategorien“ wesentlicher und wichtiger Einrichtungen festlegen, die (a) nur bestimmte zertifizierte IKT-Produkte, -Dienste und -Prozesse nutzen dürfen, oder die (b) ein Zertifikat eines EU-Schemas zur Zertifizierung der Cybersicherheit erlangen müssen.[280] Die Möglichkeit für die Kommission, solche Festlegungen eigenständig vornehmen zu dürfen, sollte überdacht werden. Im Sinne der Stärkung der demokratischen Legitimation sollten solche Entscheidungen nicht von der Kommission über delegierte Rechtsakte, sondern durch den EU-Gesetzgeber – Rat und Europäisches Parlament – (auf Level 1) getroffen werden. Dies gilt umso mehr, als der Spielraum, den die NIS-2-Richtlinie der Kommission diesbezüglich einräumt, übermäßig groß erscheint. So kann die Kommission immer dann aktiv werden, wenn „ein unzureichendes Niveau der Cybersicherheit festgestellt wurde“. Diese Formulierung wirft jedoch verschiedene Fragen auf, insbesondere, ab wann ein Cybersicherheitsniveau als „unzureichend“ zu werten ist und wer die Feststellung eigentlich vorgenommen haben muss. Auch diese Unklarheiten sollten im Rahmen einer gezielten Überarbeitung der NIS-2-Richtlinie angegangen werden. Hier böte es sich an, dass der EU-Gesetzgeber in einem ersten Schritt die Kategorien von wesentlichen und wichtigen Einrichtungen auf Level 1 festlegt. Gleichzeitig sollte die Kommission die Richtlinie alle zwei bis drei Jahre überprüfen und dabei untersuchen, ob neue Kategorien von Einrichtungen ergänzt bzw. bestehende Kategorien gestrichen werden sollten. Kommt die Kommission zu einem solchen Urteil, sollte sie einen begründeten Gesetzgebungsvorschlag zur gezielten Anpassung der Richtlinie vorlegen. Sodann sollte der EU-Gesetzgeber darüber befinden, ob die avisierte Ergänzung und/oder Streichung geboten ist und entsprechende Änderungen an der NIS-2-Richtlinie auf Level 1 in die Wege leiten.

4.4 Kurzfristige Auswege aus der Debatte um Souveränitätsanforderungen („Überbrückungsoptionen“)

Wie bereits ausgeführt, konnten sich die EU-Kommission, die ENISA, die Mitgliedstaaten und andere Akteure, die an der Entwicklung eines Cloud-Cybersicherheitszertifizierungsschemas (EUCS) beteiligt sind, bislang nicht darauf einigen, ob dieses überhaupt „Souveränitätsanforderungen“ enthalten soll und, wenn ja, wie diese ausgestaltet sein sollten. Ein Kompromiss – ein „European Common Ground“ – zeichnet sich derzeit nicht ab weshalb sich die eigentlich zentrale Verabschiedung eines solchen

[278] Einrichtungen der öffentlichen Verwaltung agieren zwar weder gewinnorientiert noch stehen sie im Wettbewerb mit anderen Verwaltungen. Das Bekenntnis zur Nutzung einheitlicher EU-Zertifizierungsstandards könnte jedoch den Datenaustausch zwischen den Verwaltungen untereinander sowie zwischen Verwaltungen und den Nutzern öffentlicher Dienste – Bürger und Unternehmen – fördern und vertrauensbildend wirken.

[279] EU-Kommission (2024b).

[280] S. Art. 24 Abs. 2 NIS-Richtlinie.

Schemas immer weiter in die Zukunft verzögert. Ein Lösungsansatz wäre es, wie oben beschrieben, zunächst ein EUCS ohne strenge Souveränitätsanforderungen zu erlassen.

Überbrückungsoption 1: Die EU-Kommission könnte, in Zusammenarbeit mit der ENISA, den Mitgliedstaaten und einschlägigen Interessenträgern, einheitliche Souveränitätsanforderungen in Form von EU-Leitlinien, gegebenenfalls inklusive eines EU-Labels, ausarbeiten, die zwar unverbindlich und nicht Teil des EUCS wären, jedoch eine wichtige Orientierung für (potenzielle) Nutzer von Cloud-Diensten bieten könnten, für die Fragen der Cloud-Souveränität wichtig sind bzw. sein sollten. Cloud-Dienste-Anbieter, die ein Interesse daran haben, „souveräne Clouds" entlang der EU-Leitlinien anzubieten, könnten sodann aktiv damit werben, die in den EU-Leitlinien vorgezeichneten Souveränitätsanforderungen zu erfüllen bzw. erfüllen zu wollen. Dies könnte auch die Einführung eines entsprechenden Labels umfassen, vor dessen Nutzung eine externe Instanz prüfen müsste, ob der Cloud-Dienste-Anbieter die entsprechenden Anforderungen erfüllt.[281] Zwar müssten Cloud-Anbieter lediglich in Leitlinien enthaltene Souveränitätsanforderungen wegen der Freiwilligkeit, die Leitlinien zu beachten, nicht zwingend erfüllen, sondern könnten auch auf eigene und/oder von den EU-Leitlinien abweichende Souveränitätskriterien zurückgreifen (wodurch allerdings die Zersplitterung des Binnenmarkts bestehen bliebe). Dennoch würde auf diese Weise gleichzeitig ein Wettbewerb um die „glaub- und vertrauenswürdigsten" Souveränitätsanforderungen eröffnet. Betrachten potenzielle Cloud-Nutzer die EU-Kriterien als glaub- bzw. vertrauenswürdig, werden sie sich am Markt durchsetzen und damit einen EU-Standard etablieren. Dann hätte man zwar nicht de jure, aber dennoch de facto eine ähnliche Situation wie unter einem EUCS mit Souveränitätsanforderungen. Betrachten die Nutzer die EU-Kriterien jedoch nicht als glaub- und vertrauenswürdig, werden sich andere – z.B. nationale, unternehmensspezifische oder brancheneigene – Kriterien im Wettbewerb behaupten, was wiederum Anlass dafür bieten würde, die in den EU-Leitlinien festgelegten Kriterien gegebenenfalls zu überarbeiten.

Überbrückungsoption 2: Alternativ oder ergänzend zu Überbrückungsoption 1 könnte die EU-Kommission auch dazu Leitlinien ausarbeiten, auf welche Weise bzw. in welcher Form Cloud-Dienste-Anbieter potenzielle Cloud-Dienste-Nutzer darüber aufklären sollten, dass ihre Cloud-Dienste bestimmte Souveränitätsanforderungen erfüllen („Transparenzinstrument"). In diesen Leitlinien könnte sie für die verschiedenen Elemente von Souveränitätsanforderungen – z.B. Vorgaben an die Datenresidenz, zur Sicherstellung der Immunität gegen Nicht-EU-Recht oder zur Unternehmenskontrolle – konkrete Hinweise geben und Beispiele für bewährte Praktiken aufzeigen. Solche Leitlinien könnten einerseits als Richtschnur dafür dienen, wie Cloud-Dienste-Anbieter ihre Dienste als „souverän" präsentieren bzw. vermarkten dürfen bzw. sollten, und andererseits (potenziellen) Nutzern von Cloud-Diensten als Hilfestellung bei der Auswahl vermeintlich „souveräner" Clouds dienen.

4.5 Langfristige Handlungsoptionen betreffend Souveränitätsanforderungen

Erweisen sich die als Überbrückungsoptionen gedachten EU-Leitlinien als erfolgreich und entwickeln sie aus sich heraus eine gewisse Marktdurchdringung („Marktakzeptanz"), könnte in einem nächsten Schritt geprüft werden, ob die in den Leitlinien vorgezeichneten „erfolgreichen" Anforderungen in ein überarbeitetes Cloud-Zertifizierungsschema integriert werden könnten. Eine solche Integration sollte entweder erfolgen, indem

[281] Da der skizzierte Schritt lediglich als Überbrückungsoption gedacht ist, könnten die Verwendung eines Labels und die externe Prüfung gegebenenfalls zunächst auch entfallen. Die Entscheidung sollte davon abhängig gemacht werden, wie lange die Überbrückungsphase mutmaßlich dauert.

- der EU-Gesetzgeber auf Level 1 – d.h. im Rahmen eines Gesetzgebungsvorhabens – die Souveränitätskriterien, die in ein Cloud-Zertifizierungsschema aufzunehmen sind, sowie die (sensiblen) Fälle, in denen diese für bestimmte Cloud-Nutzer zur Anwendung kommen sollen, selbst ausformuliert, oder
- der EU-Gesetzgeber der Kommission auf Level 1 explizit den Auftrag erteilt und sie ermächtigt, bei der Entwicklung eines Cloud-Zertifizierungsschemas – in Zusammenarbeit mit der ENISA und mittels delegierter Rechtsakte[282] – Souveränitätskriterien zu berücksichtigen; dabei sollte auf Level 1 jedoch eindeutig vorgegeben werden, welche Kategorien von Souveränitätsanforderungen – bspw. Immunität gegen Nicht-EU-Recht – in das EU-Schema Eingang finden dürfen und welche nicht.

Unabhängig davon, welche Option gewählt wird, könnten die vorgeschlagenen Änderungen in einen überarbeiteten CSA integriert werden.

4.6 Einheitliche EU-Politik bei der öffentlichen Ausschreibung von cybersicheren Cloud-Diensten

In ihren politischen Leitlinien für die Europäische Kommission 2024-2029[283] kündigte Kommissionspräsidentin von der Leyen im Sommer 2024 an, die „Richtlinie über die Vergabe öffentlicher Aufträge (Richtlinie 2014/24/EU[284])“ in der neuen Legislaturperiode überarbeiten zu wollen, um „europäischen Produkten bei der Vergabe öffentlicher Aufträge in bestimmten strategischen Sektoren den Vorzug zu geben“[285].[286] Auch Mario Draghi schlug in seinem im September 2024 veröffentlichten Wettbewerbsfähigkeits-Bericht[287] die Entwicklung einer „einheitlichen EU-weiten Politik für die Beschaffung von Cloud-Diensten durch öffentliche Verwaltungen“ vor, welche auch „Anforderungen an die Datenresidenz“ beinhalten sollten.[288,289] Entsprechend wurde auch die neue EU-Kommissarin Henna Virkkunen in ihrem bereits angesprochenen Mission Letter beauftragt, eine „EU-weite Cloud-Politik für öffentliche Ausschreibungen“ im Rahmen eines „EU Cloud Procurement Act“ zu entwickeln.[290] Erste Hinweise deuten darauf hin, dass eine solche EU-weite Cloud-Politik für öffentliche Ausschreibungen

[282] Aufgrund einer stärkeren demokratischen Rückkopplung sind delegierte Rechtsakte hier Durchführungsrechtsakte vorzuziehen.
[283] EU-Kommission (2024d), Europa hat die Wahl, Politische Leitlinien für die nächste Europäische Kommission 2024–2029, Ursula von der Leyen, Kandidatin für das Amt der Präsidentin der Europäischen Kommission, 18. Juli 2024.
[284] Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG.
[285] EU-Kommission (2024d), S. 14.
[286] Am 13. Dezember 2024 startete die Kommission auch bereits eine Konsultation zur Evaluierung der Richtlinien über die Vergabe öffentlicher Aufträge. Sie zielt darauf ab, Meinungen darüber einzuholen, ob sich die die Richtlinien 2014/23/EU, 2014/24/EU und 2014/25/EU bewährt haben. Die Kommission will prüfen, ob die Richtlinien für ihre Zwecke nach wie vor geeignet sowie angemessen und ausreichend sind, um die politischen Ziele der EU zu erreichen.
[287] EU-Kommission (2024a).
[288] Dies soll darauf abzielen das öffentliche Beschaffungswesen in allen Mitgliedstaaten anzugleichen, um Ausschreibungen zu standardisieren und die Zusammenarbeit zwischen EU-Unternehmen zu erleichtern bzw. zu fördern. Draghi plädierte jedoch für Ausnahmen in national sensiblen Bereichen (z. B. Verteidigung, Inneres und Justiz) [EU-Kommission (2024a), S. 84].
[289] EU-Kommission (2024a), S. 84.
[290] EU-Kommission (2024b).

insbesondere mit einheitlichen Ausschreibungsspezifikationen[291] und einem kuratierten „EU-Marktplatz für sichere und innovative Cloud-Dienste“[292] einhergehen und darauf abzielen soll,[293]

- die Anforderungen, mit denen sich die öffentlichen Verwaltungen in den verschiedenen EU-Mitgliedstaaten bei der Nachfrage nach Cloud-Diensten verschiedener Anbieter konfrontiert sehen, stärker zu vereinheitlichen, und
- es öffentlichen Verwaltungen zu erleichtern, diejenigen Cloud-Dienste zu identifizieren, die ihren Sicherheits- und Souveränitätspräferenzen am ehesten entsprechen.

In der Tat ist die öffentliche Auftragsvergabe ein zentrales wirtschaftspolitisches Instrumentarium und kann ein wichtiger Hebel zur Lenkung der europäischen Wirtschaft in politisch erwünschte Richtungen sein. Das wird allein dadurch deutlich, dass die Ausgaben im Rahmen der öffentlichen Auftragsvergabe jährlich einen Umfang von ca. 14% des Bruttoinlandsprodukts (BIP) der EU ausmachen.[294,295]

Bereits im Rahmen der Überarbeitung der Richtlinie über die Vergabe öffentlicher Aufträge im Jahr 2014[296] einigten sich die EU-Gesetzgeber darauf, die öffentliche Auftragsvergabe verstärkt als ein „strategisches Werkzeug“ zu nutzen, um wichtigen gesellschaftlichen Herausforderungen der EU besser gerecht zu werden.[297] So zielte die Reform insbesondere darauf ab, dass öffentliche Auftraggeber die Auftragsvergabe zu Bauleistungen, Waren und Dienstleistungen strategisch einsetzen sollten. Statt allein auf den Preis als wichtigstes Kriterium zu schauen, sollten sie verstärkt ökologische und soziale Ziele mitberücksichtigen und so die Auftragsvergabe dazu nutzen, um Innovationen voranzutreiben. Dies solle auch zur „Steigerung der Effizienz und der Qualität öffentlicher Dienstleistungen“ beitragen.[298] Zugleich sollte auch weiterhin der Grundsatz gelten, wonach die Berücksichtigung derartiger strategischer Ziele den Wettbewerb nicht „künstlich einschränken“ darf. Dies bedeutet, dass ein Vergabeverfahren nicht mit der Absicht konzipiert werden darf, bestimmte Wirtschaftsteilnehmer auf „unzulässige Weise zu bevorzugen oder zu benachteiligen“.[299]

Die nun von der Kommission vorangetriebene Idee, in bestimmten strategischen Sektoren – inklusive des Cloud-Computing-Sektors – Produkten aus der EU bei der Vergabe öffentlicher Aufträge den Vorzug geben zu wollen, zielt darauf ab, die strategische Komponente bei der öffentlichen

[291] Die EU-Kommission hat einen solchen Schritt interessanterweise bereits im Februar 2020 ist ihrer EU-Datenstrategie (s. cep**Analyse**) angekündigt. Darin heißt es, dass sie „die Entwicklung gemeinsamer europäischer Standards und Anforderungen für die Vergabe öffentlicher Aufträge für Datenverarbeitungsdienste erleichtern“ will und verweist auch auf ähnliche Schritte in den USA („FedRAMP“-Programm für die Vergabe öffentlicher Aufträge) [siehe EU-Kommission (2020a)].

[292] Auch dieser Vorschlag war bereits Teil der EU-Datenstrategie vom Februar 2020 (s. cep**Analyse**). Darin führte die Kommission aus, dass sie einen EU-Marktplatz für Cloud-Dienste für Nutzer aus dem privaten und dem öffentlichen Sektor fördern wolle, welcher bei der Auswahl von Cloud-Diensten, welche bestimmte Anforderungen bezüglich „Datenschutz, Sicherheit, Datenübertragbarkeit, Energieeffizienz und Marktpraxis“ unterstützen soll und, unter anderem dem öffentlichen Sektor „die Beschaffung alternativer Lösungen erleichtern soll [siehe EU-Kommission (2020a)].

[293] Europäisches Parlament (2024), Questionnaire to the Commissioner-designate, Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy.

[294] EU-Kommission (2017), COM(2017) 572, Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine funktionierende öffentliche Auftragsvergabe in und für Europa, 3. Oktober 2017.

[295] EU-Kommission (2024d), Europa hat die Wahl, Politische Leitlinien für die nächste Europäische Kommission 2024–2029, Ursula von der Leyen, Kandidatin für das Amt der Präsidentin der Europäischen Kommission, 18. Juli 2024.

[296] Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG.

[297] EU-Kommission (2017), S. 3.

[298] Erwägungsgründe 47, 93 und 97, Richtlinie 2014/24/EU.

[299] Art. 18, Richtlinie 2014/24/EU.

Auftragsvergabe weiter zu stärken[300] und gleichzeitig den Wettbewerb – entgegen der bisherigen Rechtslage – über eine Diskriminierung von Nicht-EU-Produkten künstlich zu beschränken.

Box 3

1) „Net Zero Industry Act“: Kriterien zur ökologischen Nachhaltigkeit und Cybersicherheit bei der öffentlichen Auftragsvergabe im Hinblick auf Netto-Null Technologien

Am 13. Juni 2024 ist die Verordnung (EU) 2024/1735 zur Schaffung eines Rahmens für Maßnahmen zur Stärkung des europäischen Ökosystems der Fertigung von Netto-Null-Technologien („Net Zero Industry Act“) in Kraft getreten. Die Verordnung gilt weitestgehend bereits seit Ende Juni 2024.

Zentrales Ziel des „Net Zero Industry Act“ ist es, den Zugang der EU zu einer sicheren und nachhaltigen Versorgung mit sogenannten Netto-Null-Technologien sicherzustellen.[301] Eine zentrale Maßnahme, mit der dieses Ziel erreicht werden soll, ist die Förderung der „Nachfrage nach nachhaltigen und widerstandsfähigen Netto-Null-Technologien durch Verfahren zur Vergabe öffentlicher Aufträge“.[302] Die Verordnung sieht dazu insbesondere vor, dass öffentliche Auftraggeber bei der Vergabe öffentlicher Aufträge **„verbindliche Mindestanforderungen an die ökologische Nachhaltigkeit“** anwenden müssen, wenn Netto-Null-Technologien Teil der Aufträge sind, oder Bauaufträge oder Baukonzessionen Netto-Null-Technologien umfassen.[303] Die Kommission muss bis Ende März 2025 einen Durchführungsrechtsakt erlassen, um die erwähnten Mindestanforderungen festzulegen.[304]

Zusätzlich müssen öffentliche Auftraggeber bei Bauaufträgen und Baukonzessionen, die Netto-Null-Technologien umfassen, mindestens eine von mehreren „Bedingungen, Anforderungen oder vertraglichen Verpflichtungen“ anwenden. Dazu zählt auch die Anforderung, dass der Auftragnehmer **die Einhaltung der geltenden Cybersicherheitsanforderungen** nachweisen muss, die in „einer Verordnung über Cyberresilienz“ vorgesehen sind. Dies kann gegebenenfalls und sofern verfügbar auch **über ein einschlägiges europäisches System zur Cybersicherheitszertifizierung** erfolgen.[305]

Der „Net Zero Industry Act“ sieht ferner die Einführung von **„Resilienzkriterien“ vor**. Dies äußert sich etwa in Vorgaben, wonach nicht mehr als 50% des EU-Angebots einer Netto-Null-Technologie aus einem einzigen Drittland stammen dürfen sollen.[306]

---

2) „Vergabetransformationspaket“ des BMWK: Kriterien für eine soziale und ökologische Beschaffung und potenzieller Ausschluss von Bietern aus Drittstaaten

Am 18. Oktober 2024 legte das Bundesministerium für Wirtschaft und Klimaschutz Referentenentwürfe zur Reform des Vergaberechts („Vergabetransformationspaket“) vor. Das Paket zielt darauf ab, öffentliche Vergabeverfahren zu vereinfachen, zu digitalisieren und zu beschleunigen sowie die öffentliche Beschaffung

[300] Im Rahmen des „Net Zero Industry Act“ haben sich die EU-Gesetzgeber bereits auf solche Schritte im Hinblick auf Nett-Null-Technologien verständigt. Und auch das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) legte im Oktober 2024 im Rahmen eines „Vergabetransformationspakets“ Vorschläge für eine strategischere Ausrichtung der öffentlichen Auftragsvergabe vor. Sie wurden in überarbeiteter Form Ende November 2024 vom Bundeskabinett verabschiedet (siehe Box 3).

[301] Art. 1 Abs. 1 Verordnung (EU) 2024/1735.

[302] Art. 1 Abs. 2 Verordnung (EU) 2024/1735.

[303] Art. 25 Abs. 1 Verordnung (EU) 2024/1735.

[304] Art. 25 Abs. 5 Verordnung (EU) 2024/1735.

[305] Art. 25 Abs. 3 lit. b Verordnung (EU) 2024/1735.

[306] Erwägungsgrund 57 und At. 25 Abs. 7 Verordnung (EU) 2024/1735.

wirtschaftlich, sozial, ökologisch und innovativ auszurichten und die Verbindlichkeit der Verfahren zu stärken.[307] Das BMWK wollte[308,309]

- die öffentliche Beschaffung nachhaltiger ausrichten. Dafür soll der Staat **sozial-ökologische Kriterien künftig als Regelfall berücksichtigen** und damit einen „Hebel für eine transformative Wirtschaft" setzen sowie zur Schaffung grüner Leitmärkte beitragen. Hierfür soll beispielsweise das Ermessen von öffentlichen Auftraggebern im Hinblick auf die Berücksichtigung sozialer und umweltbezogener Kriterien begrenzt werden (neuer § 120a GWB), und
- die Möglichkeit schaffen, dass **Bewerber und Bieter aus bestimmten Drittstaaten[310]** bei bestimmten öffentlichen Aufträgen **ausgeschlossen werden können**, um die „Sicherheit Deutschlands" zu erhöhen. Dabei geht es um Aufträge in den Bereichen (a) kritische Infrastruktur im Sinne des BSI-Gesetzes sowie (b) Verteidigung und Sicherheit (neuer § 112a GWB). Ob ein solcher Ausschluss erfolgt, soll im Ermessen des Auftraggebers stehen.[311]

Am 27.November 2024 hat nun das Bundeskabinett den Gesetzentwurf zum „Vergaberechtstransformationsgesetz" beschlossen.[312] Darin ist der **Passus zum Ausschluss von Bewerbern und Bietern aus bestimmten Drittstaaten nicht mehr enthalten.** Diese Wandlung dürfte auf das Urteil des EuGH vom 22. Oktober 2024 zurückzuführen sein, in dem der Gerichtshof entschieden hat, dass die Regelung des Zugangs von Wirtschaftsteilnehmern aus Drittstaaten zu Vergabeverfahren in den Mitgliedstaaten in die ausschließliche Zuständigkeit der EU fällt.[313,314]

Interessanterweise hat sich jedoch bisher gezeigt, dass die Nutzung der öffentlichen Auftragsvergabe für strategische Zwecke nicht von durchschlagendem Erfolg gekrönt war. Bereits 2017 hob die Kommission selbst hervor, dass der niedrigste Preis in 55% der Ausschreibungen weiterhin das „einzige Vergabekriterium" darstellt und ökologische, soziale oder die Innovation betreffende Aspekte in der Praxis nur selten Berücksichtigung finden.[315] Jüngst hob auch der Europäische Rechnungshof hervor, dass die Reformen von 2014 „keine nachweisbare Wirkung" entfaltet haben und strategische Aspekte bei öffentlichen Ausschreibungen „selten berücksichtigt" wurden. So sei „in sämtlichen Mitgliedstaaten der Großteil der Aufträge nach wie vor an den Bieter mit dem niedrigsten Angebot vergeben" worden, und der Wettbewerb sei im Betrachtungszeitraum von 2011-2021 zurückgegangen.[316] In ihrer Antwort an den Rechnungshof räumt die Kommission ein, dass „die zunehmende Komplexität des Beschaffungswesens" und die strategischere Beschaffung dazu führen, dass die Vergabeverfahren

[307] Siehe Übersicht des BMWK zum Vergabetransformationspaket.
[308] Bundesministerium für Wirtschaft und Klimaschutz (2024), Referentenentwurf des Bundesministeriums für Wirtschaft und Klimaschutz, Allgemeine Verwaltungsvorschrift zur Berücksichtigung sozialer und umweltbezogener Kriterien bei der Vergabe öffentlicher Aufträge, 18. Oktober 2024.
[309] Bundesministerium für Wirtschaft und Klimaschutz (2024), Referentenentwurf des Bundesministeriums für Wirtschaft und Klimaschutz, Entwurf eines Gesetzes zur Transformation des Vergaberechts (Vergaberechtstransformationsgesetz), 18. Oktober 2024.
[310] Das sollen all jene Drittstaaten sein, die keinen völkerrechtlich privilegierten Zugang zum öffentlichen Beschaffungsmarkt der EU besitzen.
[311] Vgl. auch W. Witte (2024) Vergabetransformation im Überblick: Das plant die Ampel, 14. Oktober 2024, abrufbar hier.
[312] Bundesregierung (2024), Transformation des Vergaberechts, Einfacher und schneller Aufträge vergeben, 27.11.2024, abrufbar hier.
[313] EuGH (2024), Rechtssache C-652/22 (Kolin Inşaat Turizm Sanayi ve Ticaret).
[314] S. dazu auch Rosenkötter, A. (2024), Kein geschützter Marktzugang für Bieter aus Drittstaaten – jetzt alles geklärt?, EuGH, Urt. v. 22.10.2024 – C-652/22 – „Kolin", abrufbar hier.
[315] EU-Kommission (2017).
[316] Europäischer Rechnungshof (2023), Sonderbericht Öffentliches Auftragswesen in der EU: Weniger Wettbewerb bei der Vergabe von Aufträgen für Bauleistungen, Waren und Dienstleistungen im Zeitraum 2011–2021, 4. Dezember 2023.

komplexer und langwieriger werden, die Angebotskosten steigen und die Beteiligung an Ausschreibungen abnimmt.[317]

Sollte die Kommission nun in der neuen Legislaturperiode vorschlagen, die strategische Flanke der öffentliche Auftragsvergabe zur Sicherung der digitalen Souveränität der EU weiter zu stärken[318] – etwa durch eine Bevorzugung europäischer Cloud-Dienste, die zudem bestimmte Cybersicherheitsanforderungen (ex- oder inklusive Souveränitätsvoraussetzungen) zu erfüllen versprechen –, sollte sie die angesprochenen Erfahrungen mit der Anwendung der bestehenden EU-Vergaberichtlinien nicht ausblenden. Aufgrund dieser Erfahrungen erscheint es nicht unwahrscheinlich, dass die Mitgliedstaaten „zusätzlichen" strategischen Gesichtspunkten– in der Praxis wenig Beachtung schenken könnten, insbesondere angesichts klammer Haushalte. Sollte dies jedoch der Fall sein, erübrigt sich die Berücksichtigung der strategischen Faktoren a priori. Ferner muss bedacht werden, dass eine solche Berücksichtigung – sofern die Mitgliedstaaten sie anwenden – zu einer weiteren Verringerung der Anzahl der möglichen Bieter auf öffentliche Aufträge führen und damit den Wettbewerb über das ohnehin schon niedrige Niveau hinaus reduzieren könnten. Dies wiederum hätte eine Verteuerung der öffentlichen Beschaffung zur Folge und birgt damit die Gefahr eines übermäßigen Einsatzes knapper Steuergelder. Schließlich dürfen drei weitere Aspekte nicht außer Acht gelassen werden: Erstens führen zusätzlich bei der Auftragsvergabe zu berücksichtigende Kriterien zu einer weiter wachsenden bürokratischen Belastung, und zwar sowohl auf Seiten der Bieter, die die weiteren Kriterien erfüllen müssen, als auch auf Seiten der öffentlichen Auftraggeber, die prüfen müssen, ob diese Kriterien auch tatsächlich erfüllt werden.[319] Zweitens birgt die Berücksichtigung zusätzlicher Aspekte, die über preisliche, ökologische, soziale und die Innovation betreffende Faktoren hinausgehen, das Risiko der Entstehung weiterer, nur schwer auflösbarer Zielkonflikte (niedriger Preis einer Cloud-Lösung vs. Cloud-Dienst mit EU-Datenlokalisierung, oder Zugang zu innovativem, ökologisch vorteilhaftem Cloud-Dienst vs. Cloud-Lösung, die gegen Nicht-EU-Recht „immun" ist). Und drittens droht eine Überfrachtung der Ausschreibungsprozesse, die die Vergabe von Aufträgen nochmal zusätzlich verlangsamen könnte.

Angesichts dieser Praxiserfahrungen, Unwägbarkeiten und möglicherweise unerwünschten Nebenwirkungen einer „strategischeren", auf die digitale Souveränität abzielenden Agenda für das öffentliche Beschaffungswesen gilt es, den avisierten Weg nur in begrenztem Maße zu beschreiten. Er sollte sich insbesondere auf jene Bereiche beschränken, bei denen die Sicherheitsinteressen der EU bzw. der Mitgliedstaaten – etwa im Hinblick auf die Datensouveränität – höher zu gewichten sind[320] als andere Faktoren wie etwa der Preis oder die innovativen Eigenschaften eines Cloud-Dienstes. In allen anderen Fällen kann die öffentliche Auftragsvergabe zwar ein entscheidender Hebel sowohl für die Entstehung als auch für die Entwicklung (neuer) Märkte – im Sinne von Leitmärkten für „souveräne" Clouds aus der EU – sein. Letztlich widerspricht die Idee der staatlich getriebenen Etablierung solcher „Leitmärkte", die mit der Bevorteilung bestimmter und der Benachteiligung anderer Unternehmen einhergeht, jedoch der freiheitlichen marktwirtschaftlichen Ordnung, da der Staat ex ante bestimmte

[317] EU-Kommission (2024e), Replies of the European Commission to the European Court of Auditors' special report, Public procurement in the EU, Less competition for contracts awarded for works, goods and services in the 10 years up to 2021.

[318] Umfragen zeigen tatsächlich ein gesteigertes Interesse zumindest der öffentlichen Verwaltung in Deutschland (a) an der Implementierung von Cloud-Lösungen in den nächsten Jahren per se (66%) und (b) an der Bedeutung von Fragen der digitalen Souveränität (95%) (zusätzliche Informationen s. hier).

[319] Damit würde schließlich auch das Ziel der neuen EU-Kommission in der beginnenden Legislaturperiode konterkariert, Verwaltungslasten abzubauen und das EU-Recht zu vereinfachen.

[320] Dazu könnten beispielsweise Geheimdienstinformationen, Steuerdaten, Gesundheitsdaten oder für verteidigungsrelevante Informationen fallen.

Marktergebnisse vorzugeben beabsichtigt. Der Hebel der öffentlichen Auftragsvergabe sollte daher nur begrenzt eingesetzt werden und sich auf eng definierte Bereiche beschränken.

Die Kommission sieht schließlich die Etablierung kuratierter „EU-Marktplätze für sichere und innovative Cloud-Dienste“ vor, damit Einrichtungen der öffentlichen Verwaltungen diejenigen Cloud-Dienste leichter identifizieren können, die ihren Sicherheits- und Souveränitätspräferenzen entsprechen.[321] Solche Marktplätze können ein sinnvolles Transparenzinstrument sein, den Einrichtungen die Entscheidungsfindung erleichtern, die praktischen Aufwände potenzieller staatlicher Auftragnehmer senken und zu einer Reduktion von Transaktionskosten beitragen. Auch können sie wettbewerbsbelebend wirken, da sie Nachfragern von Cloud-Diensten eine leichtere Vergleichbarkeit verschiedener Angebote ermöglichen. Es stellt sich jedoch die Frage, ob solche Marktplätze nicht privatwirtschaftlich organisiert, etabliert und betrieben werden könnten. Gibt es hinsichtlich der Sicherheitseigenschaften von Cloud-Diensten ein besonderes Informationsbedürfnis auf Seiten potenzieller staatlicher Cloud-Nachfrager, dürften Cloud-Anbieter ein Eigeninteresse daran haben, diese Informationen auch bereitzustellen, egal, ob auf privat organisierten digitalen Einkaufsplattformen oder anderweitig. Ein Eingreifen der Kommission bzw. des EU-Gesetzgebers wäre dann unnötig. Etwaige privatwirtschaftliche Initiativen könnten allenfalls durch unverbindliche Leitlinien oder Handreichungen flankiert werden, die mögliche Elemente solcher Marktplätze vorzeichnen. Auch sollten private Marktplatzbetreiber verpflichtet sein, die Kriterien für die Aufnahme bzw. Nichtaufnahme einzelner Cloud-Anbieter auf ihre Plattform preiszugeben. Jegliche Maßnahmen auf EU-Ebene sollten jedoch den Wettbewerb um die besten Online-Marktplätze für – cybersichere/innovative – Cloud-Dienste für öffentliche Verwaltungen nicht untergraben. Sollte die EU-Kommission dennoch an der Idee festhalten, solche Marktplätze staatlicherseits entwickeln zu wollen, sollte sie die privaten Marktplätze erstens nicht ersetzen, sondern allenfalls versuchen, sie zu ergänzen. Zweitens sollte sie dabei auf bestehenden bewährten Praktiken („best practices“) in den Mitgliedstaaten aufbauen. Kritisch zu prüfen bleibt, ob staatliche Marktplätze auf beiden Ebenen – also sowohl auf Ebene der Mitgliedstaaten als auch auf EU-Ebene – wirklich notwendig sind. Im Sinne der Stärkung des Binnenmarkts und der Entstehung wettbewerblicher und grenzüberschreitender Beschaffungsmärkte wäre eine Beschränkung auf EU-Marktplätze vorzugswürdig und würde dazu beitragen, knappe staatliche finanziellen Ressourcen zu schonen.

[321] Derzeit ist die Beschaffung über Online-Marktplätze in der Regel nicht möglich, da sich dieser Weg nicht in die übliche Struktur von Vergabeverfahren einfügt. Eine Ausnahme bietet der sogenannte „Direktauftrag“, bei dem ein Unternehmen beauftragt wird, ohne dass ein Vergabeverfahren durchgeführt wird. Mehr Details siehe hier.

5 Fazit

Am 1. Dezember 2024 hat die zweite Amtszeit von Kommissionspräsidentin von der Leyen begonnen und das frisch ernannte Kollegium der Kommissionsmitglieder hat seine Arbeit aufgenommen. Während die neue Legislaturperiode ganz unter dem Zeichen der Stärkung der Wettbewerbsfähigkeit der EU steht, hat sich die Kommission auch für die künftige EU-Cloud-Politik einiges vorgenommen, teilweise bereits für das Jahr 2025.[322] Nachdem sich die Vertreter der Kommission, der EU-Mitgliedstaaten und der ENISA in den vergangenen Jahren nicht auf einen für alle Seite zufriedenstellenden Kompromiss im Hinblick auf das EU-Schema zur Zertifizierung der Cybersicherheit von Cloud-Diensten (EUCS) einigen konnten, ist es nun dringend erforderlich, einen neuen Anlauf zu starten, um in produktiver Weise wieder aus der verfahrenen Situation herauszukommen. Dieser cep**Input** hat einige mögliche (Aus-)Wege und Handlungsoptionen aus dieser Sackgasse aufgezeigt und erste Ideen für eine künftige resiliente EU-Cloud-Politik präsentiert. Unsere Vorschläge reichen von der Notwendigkeit, Zweifel an der Sinnhaftigkeit und Zweckmäßigkeit von Souveränitätsanforderungen als Grundlage für eine glaubwürdige EU-Cloud-Politik auszuräumen, über das zwingende Erfordernis, eine gesetzliche Grundlage für die Einführung von Souveränitätskriterien in einem EU-Cybersicherheitszertifizierungsschema in einem Basisrechtsakt (d.h. auf Level 1) zu schaffen, bis hin zur Anpassung einschlägiger EU-Rechtsakte wie dem EU-Rechtsakt zur Cybersicherheit, der NIS-2-Richtlinie oder auch den EU-Vorschriften zur öffentlichen Auftragsvergabe. Zugleich hat dieser cep**Input** verdeutlicht, dass es nicht ausreicht, nur an wenigen Stellschrauben zu drehen. Stattdessen bedarf es eines ganzheitlichen, übergreifenden neuen Ansatzes, um die europäische Cloud-Politik neu aufzustellen und die Cybersicherheit in Europa im Cloud-Zeitalter zu stärken. In Zeiten wachsender geo- und sicherheitspolitischer Spannungen und zunehmender Konflikte um die globale Technologieführerschaft gilt es, die digitale Souveränität der EU aufrechtzuerhalten, zu festigen und Abhängigkeiten zu reduzieren, ohne sich jedoch dabei des Zugangs zu fortschrittlichen digitalen Diensten aus Drittstaaten zu berauben und dadurch im globalen Wettbewerb zurückzufallen.

[322] Mehr Informationen zur neuen EU-Kommission finden Sie hier.

Centrum für Europäische Politik
FREIBURG | BERLIN

Autoren:

Philipp Eckhardt, Fachbereichsleiter Finanzmärkte und Informationstechnologien
eckhardt@cep.eu

Dr. Anja Hoffmann, LL.M. Eur., Wissenschaftliche Referentin, Fachbereich Binnenmarkt und Wettbewerb
hoffmann@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Räume 4205/06 | D-10117 Berlin
Tel. + 49 761 38693-0