



Brüssel, den 4. Juni 2026
(OR. en)

Interinstitutionelles Dossier:
2026/0138 (COD)

10104/26
ADD 1

TELECOM 292
CYBER 271
MI 587
COMPET 700
IA 150
CODEC 1090

VORSCHLAG

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	3. Juni 2026
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2026) 502 annex
Betr.:	ANHÄNGE der VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Schaffung eines Rahmens für Maßnahmen zur Stärkung des europäischen Cloud- und KI-Ökosystems (Verordnung zur Cloud- und KI-Entwicklung)

Die Delegationen erhalten als Anlage das Dokument COM(2026) 502 annex.

Anl.: COM(2026) 502 annex



EUROPÄISCHE
KOMMISSION

Brüssel, den 3.6.2026
COM(2026) 502 final

ANNEXES 1 to 3

ANHÄNGE

der

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

**zur Schaffung eines Rahmens für Maßnahmen zur Stärkung des europäischen Cloud-
und KI-Ökosystems (Verordnung zur Cloud- und KI-Entwicklung)**

{SEC(2026) 502 final} - {SWD(2026) 502 final} - {SWD(2026) 503 final}

ANHANG I

GROSSE HERAUSFORDERUNGEN

1. Große Herausforderung 1: Ökologische Nachhaltigkeit, Leistung und Sicherheit der Rechenzentren der Union

Unionsweite Tests und Einführung von Technologien für Rechenzentren, die neue Maßstäbe bei der Energie- und Ressourceneffizienz setzen sollen.

Dazu zählt, eine niedrigere Kennzahl zur eingesetzten Energie (PUE) zu erreichen und eine deutlich höhere Serverauslastung zu ermöglichen. Beispiele hierfür sind:

- (1) **Senkung der durchschnittlichen Kennzahl zur eingesetzten Energie:** Verbesserung der ökologischen Nachhaltigkeit und Umweltleistung der Cloud- und Edge-Rechenzentren der Union durch die Senkung der durchschnittlichen Kennzahl zur eingesetzten Energie (PUE) auf 1,15 in der gesamten Union. Im Vordergrund steht dabei die Ermöglichung folgender Entwicklungen:
 - (a) fortgeschrittene Energieeffizienztechnologien für Rechenzentren beispielsweise in den Bereichen Kühlung und Abwärmerückgewinnung;
 - (b) Quanteninformatiktechnologien für den Betrieb von Cloud- und Recheninfrastrukturen;
 - (c) Netzintegration und fortgeschrittene Energiemanagementsysteme;
 - (d) Pilotanlagen zur Validierung energieeffizienter Technologien der nächsten Generation unter Betriebsbedingungen.
- (2) **Erhöhung der durchschnittlichen Serverauslastung von Rechenzentren:** Erhöhung der durchschnittlichen Serverauslastung in den Rechenzentren der Union auf rund 50 %, z. B. durch Integration KI-gestützter Technologien für die dynamische Steuerung der Serverauslastung, die Steuerung und Planung der Arbeitslasten im laufenden Betrieb oder das Ausgleichen der Auslastung, der Energiekosten, der thermischen Randbedingungen und der Latenzanforderungen.
- (3) **Verbesserung der Sicherheit und Resilienz von Rechenzentren:** Verbesserung der Sicherheit und Resilienz der Wertschöpfungskette der Rechenzentren und ihrer Versorgung durch die Integration von in der Union entworfener und hergestellter Halbleitertechnik und Quantentechnik sowie durch die Verbesserung ihrer Widerstandsfähigkeit gegenüber physischen Bedrohungen und Cybersicherheitsbedrohungen, einschließlich gezielter Angriffe.

2. Große Herausforderung 2: Cloud-Stacks

Aufbau durchgängiger Hardware- und Software-Cloud-Stacks, einschließlich KI-Werkzeugen, Infrastrukturen, Diensten und Verwaltungsebenen, um die kritischen Kapazitätslücken der Union zu schließen.

Dazu gehört der Aufbau von KI-Servern, die mit in der Union entworfener und hergestellter Halbleitertechnik und Quantentechnik betrieben werden, für verteilte und dezentrale Cloud- und Edge-Computing-Infrastrukturen für KI.

Pilotprogramme könnten dazu beitragen, die Fähigkeiten der europäischen offenen Cloud-Stacks in strategisch wichtigen Sektoren zu demonstrieren.

3. Große Herausforderung 3: Grenz-KI

Entwicklung der nächsten Generation multimodaler Grenz-KI-Modelle und -Systeme und wegweisender neuartiger Fähigkeiten.

Der Schwerpunkt wird auf dem Architekturentwurf und der Entwicklung multimodaler Modelle und Systeme der nächsten Generation liegen, die die Grenzen der derzeitigen algorithmischen Fähigkeiten verschieben, um eine bessere Leistung beim fortgeschrittenen logischen Schlussfolgern, beim modalitätsübergreifenden Verständnis und bei Agentenfähigkeiten zu erreichen, sowie auf der Untersuchung neuartiger Ansätze für die Modelleffizienz, die kognitive Modellierung, alternative Rechenstrukturen usw.

Mögliche Anwendungsbereiche wären die Grundlagenforschung (wie etwa wissenschaftliche Entdeckungen und komplexe Datenauswertung) sowie die Entwicklung von Weltmodellen für verbessertes Schlussfolgern, automatisierte Managementsimulationen und deren Planung.

4. Große Herausforderung 4: Physische KI

Entwicklung fortgeschrittener Modelle und Systeme für physische KI, die autonom und sicher arbeiten und eine robuste Manipulation und Navigation in unstrukturierten Umgebungen ermöglichen.

Der Schwerpunkt wird auf der gemeinsamen Konzeption von Software und den ihr zugrunde liegenden Hardware-Architekturen und auf der Kombination von Grenz-KI-Techniken mit Weltmodellen liegen, die das Schlussfolgern über physikalische Zusammenhänge (*physical reasoning*) unterstützen, um robuste Manipulations-, Navigations- und Interaktionsfähigkeiten bei minimaler menschlicher Aufsicht zu ermöglichen.

Mögliche Anwendungsbereiche wären autonome Roboter, industrielle Systeme und Drohnen, die in dynamischen realen Umgebungen betrieben werden.

5. Große Herausforderung 5: Industrielle KI

Beschleunigung der Entwicklung und Verbreitung europäischer industrieller KI in allen strategischen Sektoren der Union.

Der Schwerpunkt wird auf der Entwicklung europäischer Modelle und Systeme für industrielle KI liegen, die für hochwertige industrielle Anwendungen geeignet sind. Diese Modelle und Systeme sollten an sektorspezifische Anwendungsfälle angepasst werden können und eine sichere Einführung ermöglichen.

Die im Rahmen dieser Großen Herausforderung eingeleiteten Initiativen sollten sich auf spezialisierte Rechenressourcen und Testanlagen stützen, die erforderlich sind, um KI-Systeme in realen Umgebungen zu validieren, bevor ihre groß angelegte Einführung und Nutzung auch auf regionaler und lokaler Ebene unterstützt werden kann.

In der Automobilindustrie können diese Initiativen die Entwicklung und Einführung innovativer Softwareplattformen und KI-Modelle für das automatisierte Fahren erleichtern, während sie im verarbeitenden Gewerbe die Entwicklung spezialisierter Modelle zur Optimierung der Produktionsprozesse ermöglichen können. Weitere strategische Sektoren, die von industrieller KI profitieren könnten, sind beispielsweise Gesundheitswesen, Energie, Agrar- und Ernährungswirtschaft und Verteidigung.

6. Große Herausforderung 6: Kooperative europäische Industriemodelle

Entwicklung kooperativer europäischer Modelle und Systeme für industrielle KI in strategischen Sektoren, indem eine Zusammenarbeit im industriellen Maßstab in Europa

ermöglicht wird, ohne dass sensible Geschäftsdaten zwischen den Beteiligten offengelegt werden.

Der Schwerpunkt wird auf fortgeschrittenen Technologien, die die Wahrung der Vertraulichkeit gewährleisten, liegen. Hierzu zählen föderierte und verteilte Trainingsansätze, bei denen Algorithmen zu den Daten gebracht werden, anstatt Daten zentral zusammenzuführen, sichere Ausführungsumgebungen, auf Verschlüsselung basierende Verarbeitung, Anonymisierungs- und Pseudonymisierungstechniken, Segmentierung von Zugriffsrechten und Schutz vor der Extraktion wirtschaftlich sensibler Informationen aus trainierten Modellen.

Zu den strategischen Sektoren, die von kooperativen europäischen industriellen KI-Modellen und -Systemen profitieren könnten, zählen etwa Luft- und Raumfahrt, Pharmazie, Cybersicherheit, Mobilität, autonome Fahrzeuge und Drohnen, Energie und Verteidigung.

7. Große Herausforderung 7: Plattform für KI-Agenten

Entwicklung eines europäischen Rahmens für die Orchestrierung von KI-Agenten, der die wesentliche Middleware für den resilienten und sicheren Einsatz autonomer Agenten in großem Maßstab bereitstellt.

Der Schwerpunkt liegt auf i) der Erforschung innovativer technologischer Paradigmen, die eine wirksame Zusammenarbeit vieler KI-Agenten ermöglichen, sodass deren gemeinsame Leistung die von Einzelsystemen übertrifft, während zugleich hohe Sicherheitsstandards gewährleistet werden, sowie auf ii) der Entwicklung resilienter cloudgestützter offener Plattformen für die Steuerung von KI-Agenten in großem Maßstab.

Mögliche Anwendungsbereiche wären Gesundheitswesen (z. B. zur Unterstützung klinischer Entscheidungen und zur Koordinierung der Forschung), Cybersicherheit (z. B. zur Erkennung und Abwehr von Bedrohungen) sowie Grundlagenforschung.

8. Große Herausforderung 8: KI im öffentlichen Sektor

Entwicklung von KI-Modellen und -Systemen auf der Grundlage hochwertiger Daten des öffentlichen Sektors für kritische Bereiche (wie Gesundheitswesen, öffentliche Verwaltung, Rechtswesen und Krisenmanagement sowie öffentliche Dienste).

Der Schwerpunkt liegt auf Lösungen für öffentliche Dienste, von denen erhebliche positive Auswirkungen auf die besonders kritischen öffentlichen Dienste zu erwarten sind und die von öffentlichen Einrichtungen auf verschiedenen Verwaltungsebenen gemeinsam genutzt werden können.

Ein Ziel besteht darin, die Datenweitergabe und die Entwicklung von Grenz-KI-Modellen zwischen nationalen öffentlichen Diensten zu ermöglichen, um die Auswirkungen auf den öffentlichen Sektor in der Union insgesamt zu erhöhen, auch in Bereichen, in denen sensible Daten verarbeitet werden. Rahmenbedingungen zur Wahrung der Privatsphäre (z. B. föderiertes Lernen und Erzeugung äußerst realitätsnaher synthetischer Daten), die das Trainieren von Modellen ermöglichen, ohne die Vertraulichkeit der zugrunde liegenden Datensätze zu beeinträchtigen, und Maßnahmen zur Beschleunigung der breiten Einführung solcher Modelle, auch auf regionaler und lokaler Ebene, werden ebenfalls zur Verwirklichung dieses Ziels beitragen.

ANHANG II

KRITERIEN FÜR DIE UNIONSVERTRAUENSWÜRDIGKEITSSTUFEN

In diesem Anhang sind die Kriterien festgelegt, die Anbieter von Cloud-Computing-Diensten und deren Cloud-Computing-Dienste erfüllen müssen, um als Anbieter von Diensten der Unionsvertrauenswürdigkeitsstufen 1, 2, 3 und 4 anerkannt zu werden. Für die Zwecke der Kriterien für die Unionsvertrauenswürdigkeitsstufen 1, 2, 3 und 4 fällt „Software“ im Sinne des Artikels 3 Nummer 4 der Verordnung (EU) 2024/2847 in den Anwendungsbereich dieses Anhangs und des Anhangs III der vorliegenden Verordnung. „Hardware“ im Sinne des Artikels 3 Nummer 5 der Verordnung (EU) 2024/2847 fällt nicht in den Anwendungsbereich.

1. Unionsvertrauenswürdigkeitsstufe 1

- 1.1. Für die Unionsvertrauenswürdigkeitsstufe 1 müssen Anbieter von Cloud-Computing-Diensten die folgenden kumulativen Kriterien erfüllen:
 - (a) Der Anbieter von Cloud-Computing-Diensten ist in der Union niedergelassen.
 - (b) Infrastruktur und Anlagen des Anbieters von Cloud-Computing-Diensten, einschließlich derjenigen seiner Unterauftragnehmer, die an der Erbringung des Dienstes beteiligt sind, befinden sich in der Union, es sei denn, die öffentliche Stelle schreibt ausdrücklich etwas anderes vor.
 - (c) Die Kundendaten, einschließlich Metadaten und Telemetriedaten, die vom Anbieter von Cloud-Computing-Diensten und von den an der Erbringung des Dienstes beteiligten Unterauftragnehmern verarbeitet, gespeichert und übertragen werden, verbleiben ausschließlich in der Union – es sei denn, die öffentliche Stelle schreibt ausdrücklich etwas anderes vor – und zwar jederzeit, auch vor, während oder nach der Konfiguration oder Nutzung des Dienstes.
 - (d) Lagert der Anbieter von Cloud-Computing-Diensten die technische und operative Unterstützung oder Hilfe, einschließlich etwaiger nachträglicher Vereinbarungen über weitere Auslagerungen, an Drittanbieter außerhalb der Union aus, so werden die erforderlichen rechtlichen, technischen und organisatorischen Maßnahmen ergriffen, um die Rückverfolgbarkeit, Sicherheit und Governance dieser Tätigkeiten sicherzustellen, und diese Tätigkeiten dürfen in keiner Weise die Betriebsautonomie des Anbieters von Cloud-Computing-Diensten beeinträchtigen.
 - (e) Der Anbieter von Cloud-Computing-Diensten weist nach, dass der Dienst den neuesten Cybersicherheitsstandards entspricht.
 - (f) Der Anbieter von Cloud-Computing-Diensten gewährleistet vollständige Transparenz hinsichtlich der Beauftragung von Unterauftragnehmern. Der Anbieter von Cloud-Computing-Diensten stellt durch eine sorgfältige Prüfung seiner Unterauftragnehmer, vertragliche Verpflichtungen und eine kontinuierliche Beaufsichtigung sicher, dass diese ihren unionsrechtlichen Verpflichtungen nachkommen;
 - (g) Unterliegt der Anbieter von Cloud-Computing-Diensten der Kontrolle eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers, so stellt der Anbieter von Cloud-Computing-Diensten anhand unabhängiger Quellen sicher, dass in diesem Drittland keine Rechtsvorschriften oder Gepflogenheiten bestehen, nach denen der Anbieter von Cloud-Computing-Diensten verpflichtet wäre, den Behörden dieses Drittlands Informationen über Softwareschwachstellen zu melden, bevor bekannt wird, dass diese Schwachstellen ausgenutzt wurden.

- 1.2. Für die Unionsvertrauenswürdigkeitsstufe 1 gelten als Unterauftragnehmer im Sinne des Absatzes 1 ausschließlich Unterauftragnehmer, bei denen es sich um Dritte handelt, die in einer direkten Vertragsbeziehung mit dem Anbieter von Cloud-Computing-Diensten stehen und zur Erbringung der Cloud-Computing-Dienste beitragen.

2. Unionsvertrauenswürdigkeitsstufe 2

- 2.1. Für die Unionsvertrauenswürdigkeitsstufe 2 müssen Anbieter von Cloud-Computing-Diensten die folgenden kumulativen Kriterien erfüllen:

- (a) Der geprüfte Anbieter und die an der Erbringung des geprüften Dienstes beteiligten Unterauftragnehmer sind in der Union niedergelassen.
- (b) Infrastruktur, Anlagen und Personal des geprüften Anbieters, einschließlich derjenigen seiner Unterauftragnehmer, die an der Erbringung des Dienstes beteiligt sind, befinden sich in der Union.
- (c) Die Kundendaten, einschließlich Metadaten und Telemetriedaten, die vom geprüften Anbieter und von den an der Erbringung des Dienstes beteiligten Unterauftragnehmern verarbeitet, gespeichert und übertragen werden, verbleiben ausschließlich in der Union – es sei denn, die öffentliche Stelle schreibt ausdrücklich etwas anderes vor – und zwar jederzeit, auch vor, während oder nach der Konfiguration oder Nutzung des Dienstes.
- (d) Stellt die öffentliche Stelle fest, dass zusätzliche Anforderungen an die Personalüberprüfung und die Unionsbürgerschaft erforderlich sind, sollte der geprüfte Anbieter sicherstellen, dass Personal zur Verfügung steht, das diese Anforderungen erfüllt.
- (e) Der geprüfte Dienst erlangt ein europäisches Cybersicherheitszertifikat mindestens der Vertrauenswürdigkeitsstufe „mittel“ im Rahmen eines nach der Verordnung (EU) 2019/881 einzurichtenden europäischen Systems für die Cybersicherheitszertifizierung von Cloud-Computing-Diensten, sofern ein solches System im Rahmen der genannten Verordnung eingerichtet wurde und den Anbietern von Cloud-Computing-Diensten zur Verfügung steht. Wurde ein solches System noch nicht eingerichtet, gelten nationale Systeme für die Cybersicherheitszertifizierung, sofern diese vorhanden sind. Gibt es weder ein System für die Cybersicherheitszertifizierung auf nationaler Ebene noch auf EU-Ebene, muss der geprüfte Anbieter nachweisen, dass der Dienst die höchsten Cybersicherheitsstandards nach geltendem Unionsrecht erfüllt.
- (f) Die bei der Nutzung des geprüften Dienstes erzeugten Daten werden nicht zum Trainieren oder zur Optimierung von KI-Systemen verwendet, die von einem Drittland oder einem Rechtsträger mit Sitz in einem Drittland betrieben werden, und verlassen keinesfalls die Union.
- (g) Unterliegen der geprüfte Anbieter und die an der Erbringung des geprüften Dienstes beteiligten Unterauftragnehmer der Kontrolle eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers, so weisen sie nach, dass die erforderlichen rechtlichen, technischen und organisatorischen Maßnahmen getroffen wurden, um sicherzustellen, dass
 - i) die Kontrolle eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers über den geprüften Anbieter nicht in einer Weise ausgeübt wird, die dessen Fähigkeit zur Erbringung des Dienstes einschränkt oder

- beeinträchtigt, die Beschränkungen hinsichtlich der für die Erbringung des Dienstes erforderlichen Infrastrukturen und Anlagen und des erforderlichen Personals vorsieht oder die für die Erbringung des geprüften Dienstes erforderlichen Fähigkeiten und Standards untergräbt;
- ii) Drittländer oder in einem Drittland niedergelassene Rechtsträger keinen Zugang zu Kundendaten haben;
 - iii) jedweder Möglichkeit einer Störung der Kontinuität des Dienstes und/oder einer Verschlechterung der Dienstqualität durch ein Drittland oder einen in einem Drittland niedergelassenen Rechtsträger vorgebeugt wird;
 - iv) die Kontrolle eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers über den geprüften Anbieter nicht in einer Weise ausgeübt wird, die den geprüften Anbieter dazu verpflichtet, restriktive Maßnahmen wie Sanktionsregelungen, Embargos oder gleichwertige rechtliche oder administrative Maßnahmen eines Drittlands umzusetzen, durchzusetzen, anzuwenden oder einzuhalten, es sei denn, diese Maßnahmen sind nach dem nationalen Recht der Mitgliedstaaten oder dem Unionsrecht rechtmäßig;
- (h) Die technische und operative Unterstützung oder Hilfe im Zusammenhang mit dem geprüften Dienst, einschließlich nachträglicher Vereinbarungen über weitere Auslagerungen, wird ausschließlich innerhalb der Union veranlasst und durchgeführt.
- (i) Der geprüfte Anbieter weist nach, dass die folgenden Maßnahmen in Bezug auf die Software-Lieferkette getroffen wurden:
- i) eine vollständige und aktuelle Software-Stückliste (SBOM) im Sinne des Artikels 3 Nummer 39 der Verordnung (EU) 2024/2847 und eine Liste der ermittelten Abhängigkeiten, die für die Erbringung des Dienstes relevant sind, wurden dokumentiert und der Prüfstelle zur Verfügung gestellt;
 - ii) ist der Anbieter, Eigentümer und Lizenzgeber von Softwarekomponenten im Sinne des Artikels 3 Nummer 6 der Verordnung (EU) 2024/2847 oder Produkten ein in einem Drittland niedergelassener Rechtsträger, so werden Kontrollen durchgeführt und dokumentiert, um Fernzugriffsfunktionen zu unterbinden, die ein Gerät, ein System oder eine Software (auch durch Aktualisierungen) wesentlich manipulieren oder stören könnten, und um sicherzustellen, dass die sicherheitsrelevanten Komponenten von Softwareherstellern aus Drittländern im Sinne des Artikels 3 Nummer 13 der Verordnung (EU) 2024/2847 Quellcode-Prüfungen unterzogen werden und ein dokumentierter Migrationsplan vorliegt, falls der Software-Anbieter seinen Dienst nicht erbringen kann oder ein Drittland Beschränkungen auferlegt;
 - iii) unterliegt der Anbieter von Cloud-Computing-Diensten der Kontrolle eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers, so stellt der Anbieter von Cloud-Computing-Diensten anhand unabhängiger Quellen sicher, dass in diesem Drittland keine Rechtsvorschriften oder Gepflogenheiten bestehen, nach denen der Anbieter von Cloud-Computing-Diensten verpflichtet ist, den Behörden dieses Drittlands Informationen über Softwareschwachstellen zu melden, bevor bekannt wird, dass diese Schwachstellen ausgenutzt wurden.
- (j) Wird für die Erbringung des Dienstes Software verwendet, die mit einer quelloffenen Lizenz freigegeben wurde, so weist der geprüfte Anbieter nach, dass er geeignete

Kontrollen eingeführt und dokumentiert hat, um Fernzugriffsfunktionen oder -mechanismen zu unterbinden, die dazu eingesetzt werden könnten, ein Gerät, ein System oder eine Software wesentlich zu manipulieren oder zu stören.

- (k) Soweit der geprüfte Anbieter seine Dienste weltweit erbringt und ein Tochterunternehmen in einem Drittland hat, trifft der geprüfte Anbieter die erforderlichen Maßnahmen, um eine wirksame rechtliche, technische und organisatorische Trennung zwischen dem Mutterunternehmen in der Union und einem solchen Tochterunternehmen in einem Drittland zu gewährleisten und durchzusetzen.

- 2.2. Für die Unionsvertrauenswürdigkeitsstufe 2 gelten als Unterauftragnehmer im Sinne des Absatzes 1 ausschließlich Unterauftragnehmer, bei denen es sich um Dritte handelt, die in einer direkten Vertragsbeziehung mit dem Anbieter von Cloud-Computing-Diensten stehen und zur Erbringung des Cloud-Computing-Dienstes beitragen.

3. Unionsvertrauenswürdigkeitsstufe 3

- 3.1. Für die Unionsvertrauenswürdigkeitsstufe 3 müssen Anbieter von Cloud-Computing-Diensten die folgenden kumulativen Kriterien erfüllen:

- (a) Der geprüfte Anbieter und die an der Erbringung des geprüften Dienstes beteiligten Unterauftragnehmer sind in der Union niedergelassen.
- (b) Infrastruktur, Anlagen und Personal des geprüften Anbieters, einschließlich derjenigen seiner Unterauftragnehmer, die an der Erbringung des Dienstes beteiligt sind, befinden sich in der Union.
- (c) Die Kundendaten, einschließlich Metadaten und Telemetriedaten, die vom geprüften Anbieter und von den an der Erbringung des Dienstes beteiligten Unterauftragnehmern verarbeitet, gespeichert und übertragen werden, verbleiben ausschließlich in der Union – es sei denn, die öffentliche Stelle schreibt ausdrücklich etwas anderes vor – und zwar jederzeit, auch vor, während oder nach der Konfiguration oder Nutzung des Dienstes.
- (d) Bei dem Personal, einschließlich des Personals der Unterauftragnehmer, das an der Erbringung des geprüften Dienstes beteiligt ist, handelt es sich um Unionsbürger und das Personal muss sich erforderlichenfalls auch einer nationalen Sicherheitsüberprüfung unterziehen, deren Bescheinigung von einem Mitgliedstaat für den Umgang mit Verschlusssachen im Sinne des Artikels 2 Nummer 21 der Verordnung (EU) 2021/697 ausgestellt wird.
- (e) Der geprüfte Dienst erlangt ein europäisches Cybersicherheitszertifikat mindestens der Vertrauenswürdigkeitsstufe „mittel“ im Rahmen eines nach der Verordnung (EU) 2019/881 einzurichtenden europäischen Systems für die Cybersicherheitszertifizierung von Cloud-Computing-Diensten, sofern ein solches System im Rahmen der genannten Verordnung eingerichtet wurde und den Anbietern von Cloud-Computing-Diensten zur Verfügung steht. Wurde ein solches System noch nicht eingerichtet, gelten nationale Systeme für die Cybersicherheitszertifizierung, sofern diese vorhanden sind. Gibt es weder ein System für die Cybersicherheitszertifizierung auf nationaler Ebene noch auf EU-Ebene, muss der geprüfte Anbieter nachweisen, dass der Dienst die höchsten Cybersicherheitsstandards nach geltendem Unionsrecht erfüllt.

- (f) Die bei der Nutzung des geprüften Dienstes erzeugten Daten werden nicht zum Trainieren oder zur Optimierung von KI-Systemen verwendet, die von einem Drittland oder einem Rechtsträger mit Sitz in einem Drittland betrieben werden, und verlassen keinesfalls die Union.
- (g) Der geprüfte Anbieter und die an der Erbringung des geprüften Dienstes beteiligten Unterauftragnehmer unterliegen nicht der Kontrolle eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers. Abweichend von diesem Kriterium können ein Anbieter von Cloud-Computing-Diensten und dessen Unterauftragnehmer, die an der Erbringung des geprüften Dienstes beteiligt sind und der Kontrolle eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers unterliegen, für die Unionsvertrauenswürdigkeitsstufe 3 geprüft werden, wenn die Kommission hierzu einen Durchführungsrechtsakt gemäß Artikel 19 erlassen hat. Hat die Kommission einen Durchführungsrechtsakt nach Artikel 19 erlassen, müssen der geprüfte Anbieter und die an der Erbringung des geprüften Dienstes beteiligten Unterauftragnehmer auch nachweisen, dass die erforderlichen rechtlichen, technischen und organisatorischen Maßnahmen getroffen wurden, um sicherzustellen, dass
- i) die Kontrolle eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers über den geprüften Anbieter nicht in einer Weise ausgeübt wird, die dessen Fähigkeit zur Erbringung des Dienstes einschränkt oder beeinträchtigt, die Beschränkungen hinsichtlich der für die Erbringung des Dienstes erforderlichen Infrastrukturen und Anlagen und des erforderlichen Personals vorsieht oder die für die Erbringung des geprüften Dienstes erforderlichen Fähigkeiten und Standards untergräbt. Der geprüfte Anbieter sollte einen angemessenen Zugang zum Quellcode ermöglichen;
 - ii) Drittländer oder in einem Drittland niedergelassene Rechtsträger keinen Zugang zu Kundendaten haben;
 - iii) jedweder Möglichkeit einer Störung der Kontinuität des Dienstes und/oder einer Verschlechterung der Dienstqualität durch ein Drittland oder einen in einem Drittland niedergelassenen Rechtsträger vorgebeugt wird;
 - iv) die Kontrolle eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers über den geprüften Anbieter nicht in einer Weise ausgeübt wird, die den geprüften Anbieter dazu verpflichtet, restriktive Maßnahmen wie Sanktionsregelungen, Embargos oder gleichwertige rechtliche oder administrative Maßnahmen eines Drittlands umzusetzen, durchzusetzen, anzuwenden oder einzuhalten, es sei denn, diese Maßnahmen sind nach dem nationalen Recht der Mitgliedstaaten oder dem Unionsrecht rechtmäßig.
- (h) Die technische und operative Unterstützung oder Hilfe im Zusammenhang mit dem geprüften Dienst, einschließlich nachträglicher Vereinbarungen über weitere Auslagerungen, wird ausschließlich innerhalb der Union von in der Union ansässigem Personal und von Dritten, die nicht der Kontrolle eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers unterliegen, veranlasst und durchgeführt.
- (i) Der geprüfte Anbieter weist nach, dass die folgenden Maßnahmen in Bezug auf die Software-Lieferkette getroffen wurden:

- i) eine vollständige und aktuelle Software-Stückliste und eine Liste der ermittelten Abhängigkeiten, die für die Erbringung des Dienstes relevant sind, wurden dokumentiert und der Prüfstelle zur Verfügung gestellt;
 - ii) ist der Anbieter, Eigentümer und Lizenzgeber von Softwarekomponenten oder Produkten ein in einem Drittland niedergelassener Rechtsträger, so werden Kontrollen durchgeführt und dokumentiert, um Fernzugriffsfunktionen zu unterbinden, die ein Gerät, System oder eine Software (auch durch Aktualisierungen) wesentlich manipulieren oder stören könnten, und um sicherzustellen, dass die sicherheitsrelevanten Komponenten von Herstellern aus Drittländern Quellcode-Prüfungen unterzogen werden und ein dokumentierter Migrationsplan vorliegt, falls der Software-Anbieter seinen Dienst nicht erbringen kann oder ein Drittland Beschränkungen auferlegt;
 - iii) unterliegt der Anbieter von Cloud-Computing-Diensten der Kontrolle eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers, so stellt der Anbieter von Cloud-Computing-Diensten anhand unabhängiger Quellen sicher, dass in diesem Drittland keine Rechtsvorschriften oder Gepflogenheiten bestehen, nach denen der Anbieter von Cloud-Computing-Diensten verpflichtet ist, den Behörden dieses Drittlands Informationen über Softwareschwachstellen zu melden, bevor bekannt wird, dass diese Schwachstellen ausgenutzt wurden.
- (j) Wird für die Erbringung des Dienstes Software verwendet, die mit einer quelloffenen Lizenz freigegeben wurde, so weist der geprüfte Anbieter nach, dass er geeignete Kontrollen eingeführt und dokumentiert hat, um Fernzugriffsfunktionen oder -mechanismen zu unterbinden, die dazu eingesetzt werden könnten, ein Gerät, ein System oder eine Software wesentlich zu manipulieren oder zu stören.
- (k) Soweit der geprüfte Anbieter seine Dienste außerhalb der Union erbringt und ein Tochterunternehmen in einem Drittland hat, weist der geprüfte Anbieter nach, dass er die erforderlichen Maßnahmen getroffen hat, um eine wirksame rechtliche, technische und organisatorische Trennung zwischen dem Mutterunternehmen in der Union und einem solchen Tochterunternehmen in einem Drittland zu gewährleisten und durchzusetzen.
- 3.2. Für die Unionsvertrauenswürdigkeitsstufe 3 müssen die Unterauftragnehmer im Sinne des Absatzes 1 Unterauftragnehmer sein, bei denen es sich um Dritte handelt, die in einer direkten Vertragsbeziehung mit dem Anbieter von Cloud-Computing-Diensten stehen, zur Erbringung des Cloud-Computing-Dienstes beitragen und möglicherweise Zugang zu Verschlusssachen oder sensiblen Informationen im Sinne des Artikels 2 Nummer 22 der Verordnung (EU) 2021/697 benötigen.
- 4. Unionsvertrauenswürdigkeitsstufe 4**
- 4.1. Für die Unionsvertrauenswürdigkeitsstufe 4 müssen Anbieter von Cloud-Computing-Diensten die folgenden kumulativen Kriterien erfüllen:
- (a) Der geprüfte Anbieter und die an der Erbringung des geprüften Dienstes beteiligten Unterauftragnehmer sind in der Union niedergelassen.
 - (b) Infrastruktur, Anlagen und Personal des geprüften Anbieters, einschließlich derjenigen seiner Unterauftragnehmer, die an der Erbringung des Dienstes beteiligt sind, befinden sich in der Union.

- (c) Die Kundendaten, einschließlich Metadaten und Telemetriedaten, die nach einer Risikobewertung als sensibel eingestuft wurden und die vom geprüften Anbieter und von den an der Erbringung des Dienstes beteiligten Unterauftragnehmern verarbeitet, gespeichert und übertragen werden, verbleiben ausschließlich in der Union und zwar jederzeit, auch vor, während oder nach der Konfiguration oder Nutzung des Dienstes.
- (d) Bei dem Personal, einschließlich des Personals der Unterauftragnehmer, die an der Erbringung des geprüften Dienstes beteiligt sind, handelt es sich um Unionsbürger und das Personal muss sich erforderlichenfalls auch einer nationalen Sicherheitsüberprüfung unterziehen, deren Bescheinigung von einem Mitgliedstaat für den Umgang mit Verschlusssachen ausgestellt wird.
- (e) Der geprüfte Dienst erlangt ein europäisches Cybersicherheitszertifikat mindestens der Vertrauenswürdigkeitsstufe „hoch“ im Rahmen eines nach der Verordnung (EU) 2019/881 einzurichtenden europäischen Systems für die Cybersicherheitszertifizierung von Cloud-Computing-Diensten, sofern ein solches System im Rahmen der genannten Verordnung eingerichtet wurde und den Anbietern von Cloud-Computing-Diensten zur Verfügung steht. Wurde ein solches System noch nicht eingerichtet, gelten nationale Systeme für die Cybersicherheitszertifizierung, sofern diese vorhanden sind. Gibt es weder ein System für die Cybersicherheitszertifizierung auf nationaler Ebene noch auf EU-Ebene, muss der geprüfte Anbieter nachweisen, dass der Dienst die höchsten Cybersicherheitsstandards nach geltendem Unionsrecht erfüllt.
- (f) Die bei der Nutzung des geprüften Dienstes erzeugten Daten werden nicht zum Trainieren oder zur Optimierung von KI-Systemen verwendet, die von einem Drittland oder einem Rechtsträger mit Sitz in einem Drittland betrieben werden, und verlassen keinesfalls die Union.
- (g) Der geprüfte Anbieter und die an der Erbringung des geprüften Dienstes beteiligten Unterauftragnehmer unterliegen nicht der Kontrolle eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers.
- (h) Die technische und operative Unterstützung oder Hilfe im Zusammenhang mit dem geprüften Dienst, einschließlich nachträglicher Vereinbarungen über weitere Auslagerungen, wird ausschließlich innerhalb der Union von in der Union ansässigem Personal und von Dritten, die nicht der Kontrolle eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers unterliegen, veranlasst und durchgeführt.
- (i) Der geprüfte Anbieter weist nach, dass die folgenden Maßnahmen in Bezug auf die Software-Lieferkette getroffen wurden:
 - i) eine vollständige und aktuelle Software-Stückliste und eine Liste der ermittelten Abhängigkeiten, die für die Erbringung des Dienstes relevant sind, wurden dokumentiert und der Prüfstelle zur Verfügung gestellt;
 - ii) es wurden Maßnahmen getroffen, um die wirksame Kontrolle über die Softwarekomponenten oder Produkte aufrechtzuerhalten und es wird nachgewiesen, dass ein Drittland oder ein in einem Drittland niedergelassener Rechtsträger keine wirksame Kontrolle über die Konzeption, Entwicklung, Wartung und Weiterentwicklung dieser Komponenten oder Produkte besitzt oder ausübt. Eine wirksame Kontrolle umfasst die Fähigkeit, die technische Entwicklung, die Wartungsprioritäten, die Behebung von Sicherheitsproblemen und die langfristige Kontinuität der Komponente wesentlich zu beeinflussen.

- (j) Wird Software verwendet, die mit einer quelloffenen Lizenz freigegeben wurde, so weist der geprüfte Anbieter nach, dass er geeignete Kontrollen eingeführt und dokumentiert hat, um Fernzugriffsfunktionen oder -mechanismen zu unterbinden, die dazu eingesetzt werden könnten, ein Gerät, ein System oder eine Software wesentlich zu manipulieren oder zu stören.
 - (k) Soweit der geprüfte Anbieter seine Dienste außerhalb der Union erbringt und ein Tochterunternehmen in einem Drittland hat, weist der geprüfte Anbieter nach, dass er die erforderlichen Maßnahmen getroffen hat, um eine wirksame rechtliche, technische und organisatorische Trennung zwischen dem Mutterunternehmen in der Union und einem solchen Tochterunternehmen in einem Drittland zu gewährleisten und durchzusetzen.
- 4.2. Für die Unionsvertrauenswürdigkeitsstufe 4 gelten als Unterauftragnehmer im Sinne des Absatzes 1 ausschließlich Unterauftragnehmer, bei denen es sich um Dritte handelt, die in einer direkten Vertragsbeziehung mit dem Anbieter von Cloud-Computing-Diensten stehen, zur Erbringung des Cloud-Computing-Dienstes beitragen und möglicherweise Zugang zu Verschlusssachen oder sensiblen Informationen für die Erbringung des Dienstes benötigen.

ANHANG III

PRÜFBELEGE FÜR DAS PRÜFVERFAHREN

Die Prüfstellen sollten die in diesem Anhang aufgeführten Prüfbelege von dem geprüften Anbieter anfordern, wenn sie die Konformität des geprüften Dienstes anhand der geltenden Prüfkriterien gemäß Anhang II bewerten.

Dieser Anhang enthält keine vollständige Auflistung; die Prüfstellen können auch andere als die in diesem Anhang aufgeführten Prüfbelege anfordern oder berücksichtigen. Die Prüfer können zusätzliche Informationen anfordern, die im Rahmen von Prüfungen für eine umfassende und genaue Konformitätsbewertung erforderlich sind. Die angeforderten Belege können zwar identisch sein, die zu analysierenden Aspekte unterscheiden sich jedoch je nach den Kriterien für die Vertrauenswürdigkeitsstufen und deren Anforderungsniveau.

1. Prüfkriterium A – Niederlassung in der Union

Die Prüfstelle sollte das in Anhang II unter den Unionsvertrauenswürdigkeitsstufen 2, 3 und 4 jeweils in Buchstabe a aufgeführte Prüfkriterium anhand folgender Belege bewerten:

- (1) Jegliche Belege, aus denen hervorgeht, dass der geprüfte Anbieter nach dem Recht eines Mitgliedstaats in der Union niedergelassen oder nach dem Gesellschaftsrecht eines Mitgliedstaats in der Union gegründet wurde.
- (2) Jegliche Belege dafür, dass sich der eingetragene Sitz, die Hauptverwaltung und die Hauptniederlassung des geprüften Anbieters in der Union befinden.
- (3) Die Prüfstelle sollte den geltenden Unionsrechtsrahmen des geprüften Anbieters überprüfen und prüfen, ob es sich um eine echte und dauerhafte Niederlassung handelt oder ob der geprüfte Anbieter stattdessen lediglich als außereuropäischer Anbieter einzustufen ist, der Dienste in der Union anbietet.
- (4) Die Prüfstelle sollte prüfen, ob der Anbieter in einem Mitgliedstaat der Union rechtmäßig eingetragen ist. Als Beleg hierfür könnten unter anderem Unternehmensregistrauszüge, Bescheinigungen über die steuerliche Ansässigkeit, Gewerbescheine, die Umsatzsteuer-Identifikationsnummer, und die Überprüfung, ob der Anbieter im System zur Verknüpfung von Unternehmensregistern (BRIS) und im Mehrwertsteuer-Informationsaustauschsystem (MIAS) registriert ist, dienen.
- (5) Die Prüfstelle sollte überprüfen, ob der geprüfte Anbieter dauerhaft und tatsächlich in der Union ansässig ist. Die Prüfstelle sollte daher überprüfen, ob
 - (a) sich physische Büros oder Betriebsstätten in der EU befinden (etwa anhand von Mietverträgen, Rechnungen von Versorgungsunternehmen oder Eigentumsurkunden);
 - (b) sich ständiges Personal in der Union befindet und ob die Kundenbetreuung in der Union durchgeführt wird (etwa anhand von Arbeitsverträgen, Gehaltsabrechnungen, Arbeitszeitnachweisen);
 - (c) die Vertragsabwicklung in der Union erfolgt (etwa anhand von Aufzeichnungen über das Tätigkeitsmanagement oder über die Meldung von Vorfällen);
 - (d) Bankgeschäfts- und Buchhaltungstätigkeiten ausschließlich in der Union durchgeführt werden (etwa anhand von Jahresabschlüssen und gesetzlich vorgeschriebenen Prüfberichten).

- (6) Die Prüfstelle sollte überprüfen, ob sich Niederlassungen oder Zweigniederlassungen in den Mitgliedstaaten der Union befinden (etwa anhand von Mietverträgen, Rechnungen von Versorgungsbetrieben, Eigentumsurkunden, Arbeitsverträgen, Arbeitszeitznachweisen, Gehaltsabrechnungen oder Bestellungen).

2. Prüfkriterium B – Standort der Infrastruktur, der Anlagen und des Personals

Die Prüfstelle sollte das in Anhang II unter den Unionsvertrauenswürdigkeitsstufen 2, 3 und 4 jeweils in Buchstabe b aufgeführte Prüfkriterium anhand folgender Belege bewerten:

(1) Standort der Infrastruktur

- (a) Eine Liste mit relevanten Angaben zum Standort der Infrastruktur und der Datenspeicherstandorte, die für die Erbringung des geprüften Dienstes genutzt werden. Diese Liste sollte den genauen Standort (Nummer, Straße, Stadt, Postleitzahl und Land) der Infrastruktur enthalten und belegen, dass alle Elemente für die Erbringung des geprüften Dienstes innerhalb der Union verbleiben. Dies umfasst die Standorte der Primär-, Sicherungskopie-, Notfallwiederherstellungs- und Protokollspeicher.
- (b) Sonstige Belege dafür, dass sich die IT-Infrastruktur in der Union befindet, z. B. Mietverträge, Eigentumsurkunden, Wartungsverträge, Dienstleistungsverträge, Protokolle über den Zugang zu den Anlagen.
- (c) Netzwerkdiagramme und Architekturunterlagen, aus denen hervorgeht, dass für die Datenspeicherung und -verarbeitung ausschließlich Infrastrukturen innerhalb der Union genutzt werden, auch für die Datensicherung und Datenreplizierung.

(2) Standort der Anlagen

- (a) Eine Liste mit relevanten Angaben zu den Anlagen, die für die Erbringung des geprüften Dienstes verwendet werden, z. B. ein Anlagenverzeichnis.
- (b) Belege dafür, dass sich Server, Ausrüstung und betriebliche Anlagen in der Union befinden, wie etwa Unterlagen mit Angaben zum Server und seinem Standort, Einkaufsbelege, Lieferscheine, Lizenzvereinbarungen, Abonnementverträge oder Rechnungen für Softwarekäufe oder -abonnements, Rechnungen für Hardware mit Liefernachweisen.
- (c) Belege dafür, dass sich die Kapazitäten für die Erbringung von Diensten in der Union befinden, z. B. Bereitstellungsnachweise, Installationsnachweise, Berichte zum Dienststatus, Konfigurationsberichte, Überwachungsergebnisse, Administratorprotokolle, aus denen die Nutzung des Dienstes hervorgeht.

(3) Standort des Personals

- (a) Eine Liste mit relevanten Angaben zum Personal, das für die Erbringung des geprüften Dienstes eingesetzt wird.
- (b) Belege dafür, dass das an der Erbringung des geprüften Dienstes beteiligte Personal in der Union ansässig ist, wie etwa Arbeitsverträge, Gehaltsabrechnungen, Arbeitszeitznachweise, Tätigkeitsnachweise und Organisationspläne, aus denen das in der Union ansässige Personal und die entsprechenden betrieblichen Zuständigkeiten hervorgehen.

(4) Erwägungen in Bezug auf Infrastruktur, Anlagen und Personal

- (a) Die Prüfstelle sollte auch bewerten, wo Infrastruktur, Anlagen oder Personal

- i) Kundendaten speichern, übermitteln, abrufen, verarbeiten oder anderweitig handhaben;
- ii) den administrativen Zugang zu, die Kontrolle über, die Konfiguration von oder die Einsichtnahme in Kundendaten bereitstellen, ermöglichen oder ermöglichen könnten;
- iii) im Falle einer Beeinträchtigung, Fehlkonfiguration, Nichtverfügbarkeit oder Störung voraussichtlich eine Störung oder Nichtverfügbarkeit des geprüften Dienstes verursacht würde.

Anmerkung: „Infrastruktur“ bezeichnet physische Infrastrukturen, wie beispielsweise Rechenzentrumsinfrastrukturen oder Kolokationsinfrastrukturen, Netzwerke, Kühlsysteme und IT-Systeme, die die Verwaltung des Rechenzentrums ermöglichen.

„Anlagen“ bezeichnet Hardware und Software, wie beispielsweise Bibliotheken, das für die Kommunikation zwischen Softwarekomponenten erforderliche interne Netz und kryptografisches Material, das die Erbringung von Cloud-Computing-Diensten ermöglicht.

„Personal“, einschließlich des von Unterauftragnehmern verwalteten Personals, bezeichnet Personen, die die Erbringung, Verwaltung, Sicherheit, Verfügbarkeit oder den Betrieb des geprüften Dienstes unterstützen.

3. Prüfkriterium C – Datenlokalisierung in der Union

Die Prüfstelle sollte das in Anhang II unter den Unionsvertrauenswürdigkeitsstufen 2, 3 und 4 jeweils in Buchstabe c aufgeführte Prüfkriterium anhand folgender Belege bewerten:

- (1) Belege dafür, dass Kundendaten ausschließlich in der Union gespeichert und verarbeitet werden und dass Dritte oder Unterauftragnehmer, die die Bedingungen dieses Anhangs nicht erfüllen, unter keinen Umständen technisch oder operativ in der Lage sind, ohne vorherige Genehmigung auf Kundendaten zuzugreifen, sie zu erlangen, unzugänglich zu machen, zu vernichten oder ganz allgemein zu verarbeiten. Beispiele hierfür sind Zugriffsprotokolle, Zugriffsregelungen für Unterstützungstätigkeiten, Aufzeichnungen über privilegierte Zugriffe, Regelungen zur Aufbewahrung von Sicherheitskopien und Datenflussdiagramme, aus denen hervorgeht, wo die Kundendaten gespeichert, verarbeitet, repliziert und Sicherheitskopien von ihnen gemacht werden. Werden personenbezogene Daten verarbeitet, sind Verträge mit den Unterauftragnehmern vorzuweisen, die die Einhaltung der Verordnung (EU) 2016/679 nachweisen.
- (2) Protokolle und Überwachungsaufzeichnungen, aus denen hervorgeht, dass alle Daten ausschließlich in der Union gespeichert und verarbeitet werden. Beispiele hierfür sind Dienstleistungsrahmenverträge, Datenverarbeitungsvereinbarungen, vertragliche Datenresidenzvereinbarungen oder eine EU-Datengrenze.
- (3) Belege (wie etwa vertragliche Vereinbarungen, Protokolle und Verfahren, die öffentlichen Stellen angeboten werden), aus denen hervorgeht, dass der geprüfte Anbieter und die an der Erbringung des geprüften Dienstes beteiligten Unterauftragnehmer die erforderlichen Maßnahmen ergriffen haben, um sicherzustellen, dass
 - (a) ohne Zustimmung der öffentlichen Stelle keine Kundendaten, auch keine verschlüsselten Daten, die Union verlassen;

- (b) keine Daten an andere Dritte übermittelt werden, bei denen es sich nicht um an der Erbringung des Dienstes beteiligte Unterauftragnehmer oder um von der öffentlichen Stelle ausdrücklich berechnigte Empfänger handelt.
- (4) Ein Datenflussdiagramm, das die Datenflüsse zwischen dem Anbieter von Cloud-Computing-Diensten und den Kunden sowie mit Diensten Dritter und Unterauftragnehmern zeigt. Aus dem Diagramm müssen Ursprung und Bestimmungsort der Daten eindeutig hervorgehen wie auch ein Nachweis, dass die Daten die Union nicht verlassen.

Anmerkung: Für die Zwecke dieses Anhangs bezeichnet „Kunde“ eine öffentliche Stelle, die mit dem Anbieter von Cloud-Computing-Diensten eine vertragliche oder sonstige rechtsverbindliche Vereinbarung über den Zugang zum Cloud-Computing-Dienst oder dessen Nutzung geschlossen hat.

„Kundendaten“ können alle Daten umfassen, die unter der rechtlichen, vertraglichen oder anderweitigen Kontrolle des Kunden des Cloud-Computing-Dienstes stehen und die

- (a) vom Kunden oder in dessen Namen in den Cloud-Computing-Dienst eingegeben werden, einschließlich Authentifizierungsdaten,
- (b) erzeugt werden, indem der Nutzer den Cloud-Computing-Dienst nutzt.

Kundendaten können auch Daten umfassen, die unter der Kontrolle des geprüften Anbieters stehen und die infolge der Interaktion des Kunden des Cloud-Dienstes mit dem geprüften Dienst erlangt werden. Hierzu gehören auch Kundendaten und alle Daten, die sich aus der Nutzung der Cloud-Computing-Dienste ergeben (d. h. Telemetrie- oder Metadaten).

„Von Cloud-Computing-Diensten abgeleitete Daten“ umfassen den Teil der Protokolldaten, der Aufzeichnungen darüber enthält, wer den Dienst zu welcher Zeit und welche Funktionen genutzt hat, betroffene Arten von Daten usw. Hierzu können zudem Informationen über die Anzahl der autorisierten Nutzer und deren Identität zählen wie auch alle Konfigurations- oder Anpassungsdaten, wenn der Cloud-Computing-Dienst über solche Konfigurations- und Anpassungsfunktionen verfügt.

4. Prüfkriterium D – Unionsbürgerschaft

Die Prüfstelle sollte das in Anhang II unter den Unionsvertrauenswürdigkeitsstufen 2, 3 und 4 jeweils in Buchstabe d aufgeführte Prüfkriterium anhand folgender Belege bewerten:

- (1) Der geprüfte Anbieter sollte der Prüfstelle gegenüber nachweisen, dass er die Maßnahmen umgesetzt hat, mit denen sichergestellt wird, dass es sich bei dem an der Erbringung des geprüften Dienstes beteiligten Personal um Unionsbürger handelt, falls eine öffentliche Stelle die Unionsbürgerschaft als Voraussetzung vorschreibt. Dies kann durch gültige amtliche Dokumente (wie einen gültigen Reisepass oder Personalausweis) nachgewiesen werden.
- (2) Der geprüfte Anbieter sollte Organisationspläne und Stellenbeschreibungen vorlegen, aus denen hervorgeht, dass er auf Anfrage sicherstellen kann, dass ausschließlich Personal mit Unionsbürgerschaft mit dem Betrieb, der Verwaltung, der Wartung und der Betreuung der geprüften Dienstes betraut wird.
- (3) Der geprüfte Anbieter sollte Unterlagen vorlegen, aus denen die Konzepte für die Zugriffskontrolle sowie Prüfpfade hervorgehen, um nachzuweisen, dass nur befugte Mitarbeiter, die Unionsbürger sind, Zugang zu den Systemen und Daten des Dienstes haben.

- (4) Der geprüfte Anbieter sollte nachweisen, dass er Verfahren eingeführt hat, die regeln, wie die Staatsbürgerschaft vor einer Aufgabenzuweisung überprüft wird und wie die Einhaltung dieses Prüfkriteriums während der gesamten Beschäftigung aufrechterhalten wird.

Anmerkung: Das an der Erbringung des geprüften Dienstes beteiligte Personal könnte Personal umfassen, das logischen oder physischen Zugang zu Infrastruktur und Anlagen hat, die für den Betrieb des Cloud-Computing-Dienstes genutzt werden, sowie Personal, das für die Kundenbetreuung zuständig ist, und das gesamte Personal, das die Managementkontrolle über den Anbieter von Cloud-Computing-Diensten ausübt.

5. Prüfkriterium E – Europäisches System für die Cybersicherheitszertifizierung, gemäß der Verordnung (EU) 2019/881

Die Prüfstelle sollte das in Anhang II unter den Unionsvertrauenswürdigkeitsstufen 2, 3 und 4 jeweils in Buchstabe e aufgeführte Prüfkriterium anhand folgender Belege bewerten:

- (1) Ein gültiges europäisches Cybersicherheitszertifikat, das von einer zuständigen Konformitätsbewertungsstelle ausgestellt wurde und aus dem hervorgeht, dass der geprüfte Dienst im Rahmen eines gemäß der Verordnung (EU) 2019/881 angenommenen europäischen Systems für die Cybersicherheitszertifizierung bewertet wurde und die Anforderungen der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ oder „hoch“ erfüllt, sofern ein solches System eingerichtet wurde.
- (2) Einen Zertifizierungsbericht mit einer Beschreibung der wichtigsten Komponenten, die für die Entwicklung und den Betrieb des Cloud-Computing-Dienstes verwendet werden, der Gegenstand der Prüfbescheinigung ist.
- (3) Bis zur Einrichtung des europäischen Systems für die Cybersicherheitszertifizierung von Cloud-Computing-Diensten kann der geprüfte Anbieter die Konformität durch gültige Cybersicherheitszertifizierungen nachweisen. Hierzu zählen unter anderem:
 - (a) ein gültiges, von einer zuständigen Konformitätsbewertungsstelle ausgestelltes Zertifikat (gemäß CEN/CLC/TS 18072:2025), aus dem hervorgeht, dass der Cloud-Computing-Dienst bewertet wurde und die Anforderungen der in CEN/TS 18026:2024 festgelegten Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ oder „hoch“ erfüllt;
 - (b) ein von der jeweils zuständigen nationalen Behörde ausgestelltes gültiges Zertifikat, aus dem hervorgeht, dass der Cloud-Computing-Dienst bewertet wurde und die Anforderungen des derzeit in dem Mitgliedstaat geltenden nationalen Cybersicherheitssystems erfüllt;
 - (c) falls es ein solches nationales System nicht gibt: Belege dafür, dass die höchsten auf dem Markt verfügbaren Cybersicherheitsstandards eingehalten werden.

6. Prüfkriterium F – Von einem Drittland oder einem Rechtsträger eines Drittlands betriebene KI-Systeme

Die Prüfstelle sollte das in Anhang II unter den Unionsvertrauenswürdigkeitsstufen 2, 3 und 4 jeweils in Buchstabe f aufgeführte Prüfkriterium anhand folgender Belege bewerten:

- (1) Vertragsklauseln, in denen festgelegt ist, dass Daten, die unter Nutzung des geprüften Dienstes verarbeitet oder erzeugt werden, einschließlich von Kunden abgeleiteter Daten, Protokolle und Telemetrie, nicht zum Trainieren oder zur Optimierung von KI-Modellen oder -Systemen, die von einem Drittland oder einem

Rechtsträger aus einem Drittland betrieben werden, verwendet werden dürfen und keinesfalls die Union verlassen dürfen.

- (2) Vertragsklauseln, in denen festgelegt ist, dass Daten ausschließlich für die Erbringung des geprüften Dienstes und nicht für Dienstverbesserungen, Modell- oder Systemverbesserungen oder andere sekundäre Zwecke verarbeitet werden dürfen.
- (3) Datenflussdiagramme, mit denen der durchgehende Datenfluss, einschließlich Datenaufnahme, -speicherung, -verarbeitung und -löschung, dokumentiert wird. Aus den Diagrammen sollte auch hervorgehen, wo die KI-Pipelines oder die Vorgänge des maschinellen Lernens (MLOps) mit Kundendaten verknüpft werden.
- (4) MLOps- oder Bereitstellungsprotokolle, aus denen hervorgeht, dass sich die Standorte für Erstellung, Tests und Freigabe in der Union befinden.
- (5) Modell- oder Systemkarten, die die Modell- oder Systembezeichnung, Version, Angaben zum Training und zur Validierung enthalten, einschließlich Erklärungen, dass die bei der Nutzung des geprüften Dienstes erzeugten Daten die Union nicht verlassen.
- (6) Datenherkunftsregelungen und zugehörige Umsetzungsunterlagen, aus denen hervorgeht, dass der Anbieter Datenherkunfts- und Datenursprungstools betreibt, und aus denen (pro Protokoll) hervorgeht, wofür die Daten verwendet wurden.
- (7) Eine Liste der Unterauftragnehmer (unter Angabe des Landes ihrer Niederlassung), die auf die durch die Nutzung des geprüften Dienstes erzeugten Daten zugreifen.

7. Prüfkriterium G – Fehlende Kontrolle durch ein Drittland oder durch einen Rechtsträger aus einem Drittland

Die Prüfstelle sollte das in Anhang II unter den Unionsvertrauenswürdigkeitsstufen 2, 3 und 4 jeweils in Buchstabe g aufgeführte Prüfkriterium anhand folgender Belege bewerten:

- (1) Die Prüfstelle sollte Folgendes ermitteln und analysieren:
 - (a) alle direkten und indirekten Anteilseigner, bis hin zu den Endeigentümern;
 - (b) die Beteiligungsübersicht, aus der die Eigentumsstruktur des Unternehmens hervorgeht;
 - (c) das Organ, das befugt ist (bzw. die Organe, die befugt sind), strategische Entscheidungen zu treffen (z. B. Hauptversammlung, Aufsichtsrat, Vorstände usw.);
 - (d) die Vorschriften für die Ernennung/Wahl/Abberufung von Leitungsorganen und die tatsächliche Zusammensetzung der Leitungsorgane (z. B. um festzustellen, ob ein Anteilseigner berechtigt ist, einen Vertreter des Vorstands zu nominieren, oder über die Mehrheit der Sitze im Vorstand verfügt);
 - (e) die für die Annahme strategischer Entscheidungen erforderlichen Beschlussfähigkeiten und Mehrheiten, um festzustellen, ob ein Anteilseigner eine strategische Entscheidung treffen kann (entweder weil er über die dafür erforderliche Mehrheit verfügt oder weil er eine solche Entscheidung durch ein Veto oder andere besondere Rechte blockieren kann, selbst wenn er eine solche Entscheidung nicht allein durchsetzen kann usw.);
 - (f) den möglichen Einfluss auf strategische Entscheidungen durch Geschäftsbeziehungen, finanzielle Verbindungen oder andere Mittel usw.

- (2) Der geprüfte Anbieter sollte alle oben genannten Informationen auch von seinen Unterauftragnehmern anfordern und sie der Prüfstelle zur Verfügung stellen.

7.1. Bewertung der Eigentums- und Kontrollverhältnisse:

- (1) Der geprüfte Anbieter sollte der Prüfstelle folgende Belege in Bezug auf seinen Hauptsitz vorlegen:

- (a) Standort und vollständige Anschrift des weltweiten Hauptsitzes und/oder der Unternehmenszentrale;
- (b) die Standorte der Leitungs- und Verwaltungsstrukturen.

- (2) Der geprüfte Anbieter sollte der Prüfstelle folgende Belege in Bezug auf die Eigentumsstruktur und besondere Rechte vorlegen:

- (a) Eine detaillierte Liste, in der alle Eigentümer aufgeführt sind, die
 - i) direkt oder indirekt mindestens 5 % des Kapitals oder mindestens 5 % der Stimmrechte halten, auch durch jegliche Inhalte, Einvernehmen, Beziehungen oder Vermittler. Dies umfasst Stimmrechtsvereinbarungen zwischen Anteilseignern, die zusammen mehr als 5 % der Stimmrechte oder 5 % des Kapitals halten würden;
 - ii) über eines oder mehrere der folgenden besonderen Eigentumsrechte verfügen: a) Vetorecht bei der Übertragung von Anteilen; b) Vorkaufsrechte der Anteilseigner c) das Recht, zusätzliche Anteile zu erwerben sowie an Bedingungen geknüpfte Investitionen.

- (b) Zur Bewertung der in Absatz 2 Buchstabe a genannten Elemente sollte die Prüfstelle die folgenden zusätzlichen Unterlagen anfordern:

- i) Handelsregistrauszüge und Aktienbuch/Gesellschafterliste der Organisation sowie andere einschlägige Dokumente, aus denen die Anteilseigner und ihre Stimmrechte oder ihre prozentualen Anteile eindeutig hervorgehen;
- ii) Aktionärs-/Gesellschaftervereinbarungen, Absichtserklärungen zwischen den Anteilseignern, Satzungen, Gesellschaftsverträge oder andere relevante Dokumente zu den Entscheidungsverfahren innerhalb des Rechtsträgers, Investitionsvereinbarungen zwischen den Anteilseignern usw.;
- iii) Anteilseigner, die juristische Personen sind und mindestens 5 % des Kapitals oder mindestens 5 % der Stimmrechte halten:
 - (1) eine Grafik, in der die verschiedenen Eigentumsebenen/Kontrollketten bis hin zu den Endeigentümern dargestellt werden;
 - (2) die Gesellschaftsverträge, Satzungen oder gleichwertige Gründungsurkunden;
 - (3) ein Verzeichnis der Direktoren, Geschäftsführer und Unterzeichner.

- (3) Der geprüfte Anbieter sollte der Prüfstelle folgende Belege in Bezug auf die Unternehmensführung vorlegen:

- (a) Der geprüfte Anbieter sollte der Prüfstelle eine Beschreibung folgender Aspekte vorlegen:

- i) Entscheidungsgremien, ihre Zusammensetzung sowie Staatsangehörigkeit oder Niederlassungsort (falls zutreffend);
- ii) Vorschriften über die Wahl, Ernennung, Nominierung oder Amtszeit der Mitglieder der Entscheidungsgremien oder anderer Führungspositionen;
- iii) Entscheidungsverfahren, einschließlich Informationen über die erforderliche Mehrheiten und/oder die Beschlussfähigkeit;
- iv) interne Führungsregelungen, in denen beschrieben wird, wie Entscheidungen in Bezug auf Eigentum und Kontrolle dokumentiert und genehmigt werden;

Entscheidungen des Vorstands und der Geschäftsleitung, die die angegebene Kontrollstruktur widerspiegeln;

Sitzungsprotokolle und Beschlüsse des Vorstands über Änderungen der Kontrollstruktur.

- (b) Der geprüfte Anbieter sollte der Prüfstelle zusätzliche Unterlagen vorlegen, in denen Folgendes festgelegt oder beschrieben wird: die Entscheidungsgremien und die Vorschriften über deren Wahl, Ernennung, Nominierung oder Amtszeit, die Entscheidungsverfahren, Stimmrechte, Vetorechte, Ernennungsrechte und Genehmigungsrechte innerhalb des Rechtsträgers (z. B. Gesellschaftsverträge, Satzungen, Berichte über die Unternehmensführung usw.). Die zusätzlichen Unterlagen und Informationen sollten für jeden zwischengeschalteten Rechtsträger, der direkt oder indirekt mindestens 5 % des Kapitals oder der Stimmrechte hält, bis hin zu den Endeigentümern sämtlicher Ebenen vorgelegt werden.
- (4) Der geprüfte Anbieter sollte der Prüfstelle folgende Belege in Bezug auf die Kontrolle vorlegen:
- (a) Der geprüfte Anbieter sollte der Prüfstelle Belege für Geschäftsbeziehungen vorlegen, durch die Kontrolle ausgeübt wird. Hierzu gehören unter anderem eine Liste der natürlichen oder juristischen Personen, mit denen die geprüften Anbieter (oder die Eigentümer des geprüften Anbieters, einschließlich zwischengeschalteter Ebenen bis hin zu den Endeigentümern) eine Geschäftsbeziehung unterhalten, die a) zu einem ähnlichen Maß an Kontrolle über Geschäftsleitung und Ressourcen führt wie das Eigentum an Anteilen oder Vermögenswerten und b) von sehr langer Dauer sind (z. B. besonders wichtige langfristige Liefervereinbarungen oder von Softwareherstellern oder Kunden bereitgestellte Kredite, die mit strukturellen Verbindungen einhergehen).
 - (b) Zu den zusätzlichen Unterlagen sollten auch Kooperationsabkommen mit der öffentlichen Stelle oder mit Softwareherstellern usw. gehören.
- (5) Der geprüfte Anbieter sollte der Prüfstelle Belege für finanzielle Verbindungen vorlegen, durch die Kontrolle ausgeübt wird:
- (a) Der geprüfte Anbieter sollte die natürlichen oder juristischen Personen (einschließlich kontrollierender Anteilseigner oder Eigentümer) auflisten, von denen der geprüfte Anbieter (oder die Eigentümer) in einer Weise finanziell abhängig ist (bzw. sind), die es ihm (bzw. ihnen) ermöglichen könnte, in strategisch wichtigen Geschäftsbereichen Zugeständnisse zu erlangen.

- (b) Zu den zusätzlichen Unterlagen sollten auch Darlehensunterlagen, Satzungen und Urkunden, aus denen die finanziellen Verbindungen hervorgeht, usw.
- (6) Der geprüfte Anbieter sollte der Prüfstelle Belege zu sonstigen Kontrollmöglichkeiten vorlegen:
 - (a) Die geprüften Anbieter sollten der Prüfstelle mitteilen, ob andere Mittel, Verfahren oder Verbindungen bestehen, durch die letztlich einem anderen Drittland oder einem in einem Drittland niedergelassenen Rechtsträger die Kontrolle übertragen wird (mit einem dem Eigentum an Anteilen oder Vermögenswerten vergleichbaren Maß an Kontrolle über Geschäftsleitung und Ressourcen und von langer Dauer).
 - (b) Aus den zusätzliche Unterlagen sollte hervorgehen, dass eine solche Kontrolle besteht, oder es sollte eine Erklärung enthalten sein, dass keine solche Kontrolle besteht (diese Erklärung kann vom Vorstand des Diensteanbieters vorgelegt werden).

Anmerkung: Bei der Bewertung der Kontrolle sollten die Eigentumsstrukturen und besonderen Rechte, die Unternehmensführung, kontrollbegründende Geschäftsbeziehungen, kontrollbegründende finanzielle Verbindungen sowie sonstige Kontrollmöglichkeiten berücksichtigt werden.

7.2. Weitere Schritte ausgehend von den Ergebnissen der Beurteilung von Eigentum und Kontrolle

Stellt die Prüfstelle fest, dass der geprüfte Anbieter der Kontrolle eines Drittlands oder eines Rechtsträgers aus einem Drittland unterliegt, sollte sie folgende zusätzliche Belege anfordern:

- (c) den Nachweis dafür, dass die Kommission einen Beschluss gemäß Artikel 19 in Bezug auf das Drittland erlassen hat, dessen Kontrolle der Anbieter von Cloud-Computing-Diensten unterliegt;
- (d) sämtliche Belege dafür, dass der geprüfte Anbieter und alle an der Erbringung des geprüften Dienstes beteiligten Unterauftragnehmer die erforderlichen Maßnahmen getroffen haben, um eine wirksame rechtliche, technische und organisatorische Trennung zwischen dem Anbieter von Cloud-Computing-Diensten und einem Drittland oder einem in einem Drittland niedergelassenen Rechtsträger durchzusetzen und um sicherzustellen, dass der Anbieter von Cloud-Computing-Diensten rechtlich, technisch und operativ nicht in der Lage ist, einem Verlangen nach Zugang zu Kundendaten, einschließlich verschlüsselter Daten, nachzukommen, die Kontinuität des Dienstes zu stören oder die Dienstqualität zu verschlechtern;
- (e) sämtliche Belege dafür, dass die öffentliche Stelle über ein solches Verlangen unterrichtet wird, und eine Bestätigung, dass das Verlangen abgelehnt wurde;
- (f) sämtliche Belege dafür, dass ein aktuelles Verzeichnis sämtlicher Verlangen eines Drittlands oder eines in einem Drittland niedergelassenen Rechtsträgers nach Zugang zu Kundendaten, Störung der Kontinuität des Dienstes oder Verschlechterung der Dienstqualität geführt wird, das mindestens das Verlangen und die Antwort darauf enthält.

8. Prüfkriterium H – Keine technische und operative Unterstützung außerhalb der Union

Die Prüfstelle sollte das in Anhang II unter den Unionsvertrauenswürdigkeitsstufen 2, 3 und 4 jeweils in Buchstabe h aufgeführte Prüfkriterium anhand folgender Belege bewerten:

- (1) Belege dafür, dass der geprüfte Anbieter verbindliche Vertragsklauseln umgesetzt hat, nach denen sämtliche Tätigkeiten in Bezug auf Unterstützung, Verwaltung, Wartung, Überwachung, Sicherheitsvorfälle sowie operative Tätigkeiten ausschließlich in der Union veranlasst und durchgeführt werden müssen. Hierzu können Vertragsklauseln gehören, nach denen alle Unterauftragnehmer und Standorte, an denen Unterstützungsdienste erbracht werden, vorab mitgeteilt werden müssen, vor der Beauftragung neuer Unterauftragnehmer eine vorherige schriftliche Genehmigung einzuholen ist und das Recht besteht, außerhalb der Union niedergelassene Unterauftragnehmer abzulehnen;
- (2) Belege dafür, dass der geprüfte Anbieter ein stets aktuelles Verzeichnis der Unterauftragnehmer führt;
- (3) Belege dafür, dass der geprüfte Anbieter solche Tätigkeiten nicht an Unterauftragnehmer außerhalb der Union vergibt oder überträgt;
- (4) Belege dafür, dass der geprüfte Anbieter die erforderlichen rechtlichen, technischen und organisatorischen Maßnahmen getroffen hat, um sicherzustellen, dass bei dem geprüften Dienst kein Fernzugriff für technische und operative Unterstützung von außerhalb der Union möglich ist.
- (5) Belege dafür, dass Helpdesk- und Unterstützungsdienste des geprüften Anbieters sowie seine Infrastrukturverwaltung, der Betrieb seines Sicherheitseinsatzzentrums (SOC) oder seiner Netzbetriebszentrale (NOC), die privilegierten Zugriffe, die Handhabung von Sicherungskopien und die Notfallwiederherstellungsvorgänge des geprüften Dienstes ausschließlich in der Union geleistet bzw. durchgeführt werden, einschließlich des Zugangswegs für den Betrieb des Dienstes;
- (6) Belege dafür, dass der geprüfte Anbieter sicherstellt, dass das Personal nach dem Verlassen des Unternehmens keinen weiteren Zugang zu dem geprüften Dienst mehr hat, und sämtliche Zugriffsberechtigungen widerrufen werden;
- (7) Belege dafür, dass der geprüfte Anbieter die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um sicherzustellen, dass der administrative Zugang zu den Systemen, die für den Betrieb des geprüften Dienstes verwendet werden, über Zugangswege innerhalb der Union gewährt wird. Dies kann durch die Umsetzung einer geografisch begrenzten Netzsteuerung, eine in der Union angesiedelte Verwaltungsinfrastruktur, Kontrollen der Verwaltung des privilegierten Zugangs wie auch Überwachungsmechanismen nachgewiesen werden;
- (8) Belege dafür, dass der geprüfte Anbieter über Verfahren verfügt, mit denen sichergestellt wird, dass keine wirksame Kontrolle durch ein Drittland oder einem in einem Drittland niedergelassenen Rechtsträger besteht, auch im Falle einer nachträglichen weiteren Auslagerung.

9. Prüfkriterium I – Gewährleistung der Transparenz der Software-Lieferkette

Die Prüfstelle sollte das in Anhang II unter den Unionsvertrauenswürdigkeitsstufen 2, 3 und 4 jeweils in Buchstabe i aufgeführte Prüfkriterium anhand folgender Belege bewerten:

- (1) Der geprüfte Anbieter sollte der Prüfstelle eine vollständige und aktuelle Software-Stückliste für alle Softwarekomponenten, einschließlich quelloffener Software, zur Verfügung stellen.

- (2) Der geprüfte Anbieter sollte der Prüfstelle eine Liste der Abhängigkeiten zur Verfügung stellen. Diese sollte Folgendes umfassen:
- (a) alle verwendeten Softwaremodule, Bibliotheken oder Anwendungsprogrammierschnittstellen (API) sowie alle Entwicklungswerkzeuge;
 - (b) Herkunft der Software: wo (Herkunftsland) und von wem die Software konzipiert, entwickelt und gewartet wird, der Vertriebsstandort, für den Vertrieb der Software maßgebliche Rechtsordnung und Aktualisierungen;
 - (c) Grad der Abhängigkeit von außereuropäischen Anbietern oder Einrichtungen oder von proprietären Technologien; für Stufe 3: Belege dafür, dass keine ungerechtfertigten Lizenzbeschränkungen bestehen, wenn der Software-Stack von einem Rechtsträger aus einem Drittland bereitgestellt wird;
 - (d) Grad der Abhängigkeit von quelloffener Software;
 - (e) Nachvollziehbarkeit der gesamten Kette der Softwarehersteller und -unterhersteller, einschließlich der Prüfrechte.

Anmerkung: Die vorstehend genannten Anforderungen bedeuten, dass Gemeinschaftsunternehmen, die sich z. B. aus einem Rechtsträger der Union und einem in einem Drittland niedergelassenen Rechtsträger zusammensetzen, für diese Stufe infrage kommen können.

- (3) Der geprüfte Anbieter sollte Folgendes vorlegen:
- (a) Belege für ein risikobasiertes Verfahren zur Ermittlung und Minderung von Abhängigkeiten von externen Softwareherstellern, die für den Betrieb des Cloud-Computing-Dienstes relevant sind;
 - (b) Belege dafür, dass er eine oder mehrere alternative Softwarelösungen, einschließlich quelloffener Software, ermittelt hat. Kann keine gleichwertige Softwarelösung ermittelt werden, muss eine Lösung gefunden werden, die ein Mindestmaß an verfügbaren Funktionen gewährleistet. Es müssen Tests durchgeführt und es muss ein Umstellungsplan aufgestellt werden, der die Migration zu solchen alternativen Lösungen ermöglicht;
 - (c) Belege dafür, dass der geprüfte Anbieter im Falle eines Mangels oder Ausfalls des Software-Anbieters oder von Beschränkungen durch ein Drittland oder einen in einem Drittland niedergelassenen Rechtsträger zu einer alternativen Lösung migrieren kann;
 - (d) eine Liste offener Standards, die als Teil der Regelungen der geprüften Anbieter in Bezug auf den geprüften Dienst befolgt werden;
- (4) Der geprüfte Anbieter sollte durch Fernzugriff und Nachprüfbarkeit des Quellcodes für Transparenz sorgen, indem er
- (a) der Prüfstelle eine Liste von Belegen zur Verfügung stellt, aus denen hervorgeht, dass keine Fernzugriffsfunktionen oder -mechanismen verwendet werden, die dazu eingesetzt werden könnten, ein Gerät, ein System oder eine Software wesentlich zu manipulieren oder zu stören. Diese sollte Folgendes umfassen:
 - i) Belege für die Tests von Softwarekomponenten, wodurch verhindert werden soll, dass Fernzugriffsfunktionen oder -mechanismen

verwendet werden, die dazu eingesetzt werden könnten, ein Gerät, ein System oder eine Software wesentlich zu manipulieren oder zu stören (Testverfahren, Testberichte, Testplan usw.);

- ii) Belege dafür, dass die Änderungsmanagementverfahren der Organisation alle Firmware- und BIOS-Änderungen, Softwareaktualisierungen sowie die Integration neuer Komponenten umfassen, um den Einsatz von Fernzugriffsfunktionen oder -mechanismen zu unterbinden;
 - iii) Belege dafür, dass das Wartungsverfahren aktualisiert wird, um den Einsatz von Fernzugriffsfunktionen oder -mechanismen zu unterbinden, die dazu eingesetzt werden könnten, ein Gerät, ein System oder eine Software wesentlich zu manipulieren oder zu stören.
- (b) Der geprüfte Anbieter muss sicherstellen, dass dem unabhängigen externen Prüfer das Recht eingeräumt wird, auf den Quellcode einer solchen Software zuzugreifen und diesen zu prüfen. Der geprüfte Anbieter muss sicherstellen, dass der Prüfstelle sämtliche für die Bewertung und Prüfung des Quellcodes erforderlichen Unterlagen, technischen Materialien und Informationen vollständig, richtig und in einem zugänglichen Format zur Verfügung gestellt werden.

10. Prüfkriterium J – Quelloffene Software

Die Prüfstelle sollte das in Anhang II unter den Unionsvertrauenswürdigkeitsstufen 2, 3 und 4 jeweils in Buchstabe j aufgeführte Prüfkriterium anhand folgender Belege bewerten:

- (1) Der geprüfte Anbieter sollte durch Fernzugriff und Nachprüfbarkeit des Quellcodes für Transparenz sorgen, indem er
- (a) der Prüfstelle eine Liste von Belegen zur Verfügung stellt, aus denen hervorgeht, dass keine Fernzugriffsfunktionen oder -mechanismen verwendet werden, die dazu eingesetzt werden könnten, ein Gerät, ein System oder eine Software wesentlich zu manipulieren oder zu stören. Diese sollte Folgendes umfassen:
 - i) Belege für die Tests von Softwarekomponenten, wodurch verhindert werden soll, dass Fernzugriffsfunktionen oder -mechanismen verwendet werden, die dazu eingesetzt werden könnten, ein Gerät, ein System oder eine Software wesentlich zu manipulieren oder zu stören (Testverfahren, Testberichte, Testplan usw.);
 - ii) Belege dafür, dass die Änderungsmanagementverfahren der Organisation alle Firmware- und BIOS-Änderungen, Softwareaktualisierungen sowie die Integration neuer Komponenten umfassen, um die Einsatz von Fernzugriffsfunktionen oder -mechanismen zu unterbinden;
 - iii) Belege dafür, dass das Wartungsverfahren aktualisiert wird, um den Einsatz von Fernzugriffsfunktionen oder -mechanismen zu unterbinden, die dazu eingesetzt werden könnten, ein Gerät, ein System oder eine Software wesentlich zu manipulieren oder zu stören.
- (2) Der geprüfte Anbieter sollte Folgendes vorlegen:

- (a) Nachweis eines risikobasierten Prozesses zur Ermittlung und Minderung folgender Risiken: i) schwaches Ökosystems und schwache Gemeinschaftsunterstützung für quelloffene Software, ii) keine kontinuierliche Überwachung der veröffentlichten Aktualisierungen, iii) Verwendung quelloffener Software, die als veraltet gilt oder nicht mehr gepflegt wird;
 - (b) Belege dafür, dass der geprüfte Anbieter aktuelle Versionen der quelloffenen Software ohne unangemessene Verzögerung einsetzt;
 - (c) Belege dafür, dass der geprüfte Anbieter eine oder mehrere alternative quelloffene Lösungen ermittelt hat. Kann der geprüfte Anbieter keine gleichwertige Software ermitteln, muss er eine Lösung finden, die ein Mindestmaß an verfügbaren Funktionen gewährleistet. Der geprüfte Anbieter muss Tests durchführen und einen Umstellungsplan aufstellen, der die Migration zu alternativen Lösungen ermöglicht.
- (3) Verwendet der geprüfte Anbieter Software, die im Rahmen einer quelloffenen Lizenz freigegeben wurde, sollte er Mechanismen einrichten, um festzustellen, ob die Software von einem Drittland oder einem in einem Drittland niedergelassenen Rechtsträger (oder einer Stiftung) übernommen wird oder unter deren Kontrolle gerät, und die öffentliche Stelle hierüber rechtzeitig zu unterrichten.

11. Prüfkriterium K – Weltweite Dienste und Tochterunternehmen in Drittländern

Die Prüfstelle sollte das in Anhang II unter den Unionsvertrauenswürdigkeitsstufen 2, 3 und 4 jeweils in Buchstabe k aufgeführte Prüfkriterium anhand folgender Belege bewerten:

- (1) Die Prüfstelle sollte prüfen, dass das Tochterunternehmen rechtlich und operativ unabhängig vom geprüften Anbieter ist.
- (2) Der geprüfte Anbieter muss nachweisen, dass das Tochterunternehmen keinen Zugang zu Systemen hat, in denen Kundendaten verarbeitet oder gespeichert werden.
- (3) Der geprüfte Anbieter muss nachweisen, dass das Tochterunternehmen über keine privilegierten Konten in den Produktionsumgebungen der Union verfügt, einschließlich in den Bereichen Cloud-Verwaltung, Identitäts- und Zugriffsmanagement (IAM), Verwaltung privilegierter Zugänge (PAM), Überwachungs- oder Datenbankverwaltungsrechte.
- (4) Die Prüfstelle sollte prüfen, dass das Personal des Tochterunternehmens keinen Zugang zu Kundendaten in der Union erlangen kann.
- (5) Die Prüfstelle sollte prüfen, dass das Tochterunternehmen nicht befugt ist, das in der Union tätige Personal anzuweisen, Kundendaten offenzulegen oder Sicherheitsverfahren zu umgehen.
- (6) Die Prüfstelle sollte prüfen, dass alle bei dem Tochterunternehmen eingehenden Verlangen ausländischer Behörden förmlich an die zuständige Stelle in der Union zur rechtlichen Bewertung nach dem Unionsrecht und dem Recht der Mitgliedstaaten weitergeleitet werden.