Stellungnahme zum Cloud and AI Development Act (CADA):

Sehr geehrte/r...,

im Vorfeld des Digitalgipfels kommende Woche schicke ich Ihnen im Anhang die **Stellungnahme der Open Source Business Alliance zum CADA sowie konkrete Änderungsvorschläge und Formulierungshilfen von APELL**, dem Dachverband der europäischen Open-Source-Unternehmensverbände.

Unsere CADA-Stellungnahme ist auch auf der OSBA-Webseite zu finden: https://osb-alliance.de/pressemitteilungen/souveraene-europaeische-cloud-und-ki-nur-mit-open-source-moeglich

Unsere Position: Der Entwurf der EU-Kommission bleibt deutlich hinter den Zielen zurück, die sich die Kommission selbst gesetzt hat. Open Source muss im CADA eine zentralere Rolle spielen, damit Europa bei Cloud und KI im Wettbewerb vorne mitspielen kann.

Wie handlungs- und leistungsfähig ein Wirtschaftsstandort ist, entscheidet sich nicht nur an Kapazitäten für Rechenzentren, KI und Clouddiensten, sondern auch daran, wie viel Kontrolle und Gestaltungsfähigkeit wir bei den entsprechenden Technologien haben.

Die EU-Kommission sagt selbst, dass übermäßige technologische Abhängigkeiten Europa strategisch schaden. Umso unverständlicher ist es, dass der CADA genau beim Ausbau von Open-Source-Infrastrukturen zögert und unverbindlich bleibt.

Wer sichere und souveräne KI will, braucht Transparenz, Kontrolle und souveräne Clouds, und die gibt es nur mit Open Source.

Wie dringend klare Vorgaben für echte digitale Souveränität durch Open Source sind, zeigen zwei aktuelle Beispiele: die KI-Partnerschaft der Bundesregierung mit Nvidia und die geplante Geheimdienst-Cloud auf Google-Basis, über die NDR und WDR berichten. Beide gelten als souverän, doch wer am Ende wirklich die Software und die Updates kontrolliert, bleibt offen.

Der Digital-Gipfel in Berlin ist die Gelegenheit, verbindliche Vorgaben für Open Source auf Bundes- und EU-Ebene mit den Teilnehmenden aus ganz Europa zu diskutieren.

Wir sind ab Montag auf dem Digitalgipfel und stehen sowohl vor Ort als auch per Mail jederzeit für Rückfragen und Austausch zur Verfügung.

Mit freundlichen Grüßen

Open Source Business Alliance

Bundesverband für digitale Souveränität e.V.

Stellungnahme der Open Source Business Alliance

zum

Entwurf der EU-Kommission für einen Cloud and AI Development Act (CADA)

29. Oktober 2026

Die **Open Source Business Alliance (OSBA) – Bundesverband für digitale Souveränität e.V.** ist der Verband der Open-Source-Industrie in Deutschland und vertritt über **290 Mitgliedsunternehmen**. Die OSBA setzt sich als größter Open-Source-Verband Europas dafür ein, die zentrale Bedeutung von Open Source Software und offenen Standards für einen erfolgreichen digitalen Wandel im öffentlichen Bewusstsein nachhaltig zu verankern.

Kontakt:

Open Source Business Alliance – Bundesverband für digitale Souveränität e.V.
Pariser Platz 6a
10117 Berlin

Miriam Seyffarth
Leiterin Politische Kommunikation
Tel.: +49 (0) 30 20 65 39 221
E-Mail: seyffarth@osb-alliance.com
Internet: www.osb-alliance.com

Summary

Der Entwurf für den Cloud and AI Development Act (CADA) ist Teil des Tech Sovereignty Package der EU-Kommission und verfolgt das strategische Ziel, die digitale Souveränität Europas zu stärken.

Als größter Open-Source-Unternehmensverband in Europa und als Bundesverband für digitale Souveränität begrüßen wir das Engagement der EU-Kommission in diesem Bereich.

In dem den CADA begleitenden Dokument „Communication on European Tech Sovereignty and EU Open Source Strategy“ macht die Kommission deutlich, dass „übermäßige technologische Abhängigkeiten strategische Nachteile“ für die EU geschaffen haben. Wir teilen die Einschätzung, dass vor dem Hintergrund einer volatilen internationalen Lage und digitaler Abhängigkeiten entschlossene Schritte unternommen werden müssen. Wir begrüßen daher auch, dass die EU-Open-Source-Strategie ein strategisches Element des Tech Sovereignty Package ist.

Denn **der Einsatz von Open Source Software baut bestehende digitale Abhängigkeiten und Lock-In-Effekte ab und stärkt die digitale Souveränität der EU**, indem Wechselfähigkeit, Gestaltungsfähigkeit und Einfluss auf Hersteller ermöglicht wird.

Der Einsatz von Open Source Software

- stärkt die **Wettbewerbs- und Innovationsfähigkeit der EU** durch kürzere Innovationszyklen, schnelleren Martkeintritt, mehr Start-Up-Gründungen, gemeinsam aufgebaute offene und interoperable digitale Infrastrukturen und Cost-Sharing-Effekte, da immer wieder auf bereits vorhandenen und frei verfügbaren Software-Komponenten aufgebaut werden kann.
- stärkt die **Resilienz und die innere und äußere Sicherheit der EU** sowie die **wirtschaftliche Unabhängigkeit**, da Software-Quellcode und Know-How frei verfügbar sind und hiermit resiliente digitale Infrastrukturen sowie Kompetenzen aufgebaut werden können.
- stärkt **Transparenz und demokratische Teilhabe sowie Mitgestaltung**, da alle sich an der Entwicklung und Nutzung der Software beteiligen, ihre Anforderungen einbringen und die Software nach den eigenen Bedürfnissen anpassen und Wissen und Software frei miteinander teilen können.

- ermöglicht eine **nachhaltige Digitalisierung**, da eine einmal entwickelte Software von anderen Behörden, der Privatwirtschaft, Wissenschaft und Zivilgesellschaft nachgenutzt werden kann, statt dass Organisationen parallel immer wieder Ressourcen in die Entwicklung der gleichen Lösungen stecken müssen („Public Money, Public Code"). Die beliebig häufige Wiederverwendung von einmal erstelltem Softwarecode, die OpenSource Software ermöglicht, spart Zeit, Geld und CO2.

Damit die Unternehmen erfolgreich sein können, die zu einem wirtschaftlich nachhaltigen, souveränen, digitalen Ökosystem beitragen, brauchen wir eine **stärkere Nachfrage nach Open Source Software** und klare Vorgaben zur Beschaffung von Open-Source-Lösungen.

Die Investition in Open-Source-Produkte und -Dienstleistungen sowie in die entsprechenden Unternehmen, die diese bereitstellen, bedeutet eine **Investition in ein vertrauenswürdiges Ökosystem**, das sich für die Einhaltung von Gesetzen und Richtlinien einsetzt und nachhaltig Veränderungen und Innovationen vorantreibt. Dazu gehören auch Open-Source-Stewards und gemeinwohlorientierte Organisationen, die Entwicklungsprozesse koordinieren, unterschiedliche Akteure vernetzen und die langfristige Pflege und Nachnutzung von Open-Source-Lösungen sicherstellen. Auch diese Strukturen benötigen eine verlässliche Finanzierung und müssen bei europäischen Regulierungsmaßnahmen berücksichtigt werden.

Open Source ist ein Geschäftsmodell, mit dem Abhängigkeiten verringert und die Kontrolle über digitale Technologien erhöht werden können: vom Hardware-Design und der Softwareentwicklung über Netzwerke, Daten und Rechenzentrumsinfrastruktur bis hin zu neuen Technologien wie Künstlicher Intelligenz.

Wir begrüßen das Vorhaben der EU-Kommission, die digitale Souveränität durch die im CADA vorgeschlagenen Maßnahmen zu stärken, allerdings **wurden diese Regelungen stark verwässert** und stehen nicht im Einklang mit den in der „Communication on European Tech Sovereignty and EU Open Source Strategy" dargelegten ehrgeizigen Zielen für mehr Open Source sowie den Überschriften der einzelnen Artikel im CADA wie beispielsweise „Open Source First".

Deswegen sind erhebliche Änderungen am CADA erforderlich.

Nur mit Open Source Software und offenen Standards sind alle Stufen digitaler und technologischer Souveränität erreichbar. Dies muss sich in einem ehrgeizigen Ökosystemansatz widerspiegeln.

Im Folgenden gehen wir auf einige Aspekte im CADA ein, die aus unserer Sicht noch einer Verbesserung bedürfen.

Wir verweisen in diesem Zusammenhang auch auf die angehängten konkreten Änderungsvorschläge und Formulierungshilfen von APELL, dem Dachverband der europäischen Open-Source-Unternehmensverbände.

1. Abbau von Abhängigkeiten

Eines der Hauptziele des CADA und der übergeordneten Strategie zur technologischen Souveränität ist der Abbau der europäischen Abhängigkeiten von kritischen Technologien (Art. 1(1)(d)), was sich auch im „operational objective 2“ der „Cloud and AI Leadership Initiatives“ widerspiegelt (Art. 3(2)(b)).

Open Source als Geschäftsmodell gewährt den Nutzenden die Freiheit, die Software zu nutzen, zu untersuchen, zu teilen und zu verändern. Die Software wird also nicht als „Black Box“ bereitgestellt sondern ist transparent und anpassbar, deswegen entstehen keine Abhängigkeiten von einem einzelnen Anbieter. Mit Open Source kann die Software auch unabhängig vom ursprünglichen Hersteller weiter entwickelt, betrieben und gepflegt werden, so dass die Nutzung der Software auch dann noch möglich ist, wenn mit dem ursprünglichen Hersteller keine vertragliche Vereinbarung mehr möglich ist.

Änderungsvorschläge:

- ➔ „Open cloud computing stacks“ und „open-source middleware platforms“ werden im „operational objective 2“ ausdrücklich als strategisches Mittel erwähnt (Art. 3(1)(a) und Art. 4(2)(c)), sie müssen jedoch auch bei der Entwicklung und dem Einsatz von Rechenzentrums-Technologien (objective 1, Art. 3(2)(a)) sowie bei der Entwicklung von wegweisenden KI-Fähigkeiten (Art. 4(3)) als Standard gelten und entsprechend ergänzt werden.
- ➔ Artikel 6 zur „Implementation of the Cloud and AI Leadership Initiatives“ sowie Artikel 7 zu den „National cloud and AI strategies“ müssen eindeutig widerspiegeln, dass die operativen Ziele aus Art. 3

in den Umsetzungen auf allen Ebenen zum Tragen kommen müssen, insbesondere die Ziele mit Bezug zu offenen Technologien.

2. Ausbau von Rechenzentrumskapazitäten ohne Lock-In-Effekte

Bei der Festlegung von „data centre acceleration zones“ und der Ausweisung strategischer Projekte (Art. 10) dürfen die EU-Kommission und die Mitgliedstaaten die Bemühungen um den Abbau von Abhängigkeiten und die Stärkung der digitalen Souveränität nicht gefährden.

Änderungsvorschläge:

- ➔ Vorrang sollten diejenigen Rechenzentrumsbetreiber erhalten, die auf offenen Cloud-Stacks aufbauen und sich nach besten Kräften bemühen, proprietäre Komponenten auf allen Ebenen des Stacks zu vermeiden.
- ➔ Open-Source-Technologien müssen Vorrang erhalten.
- ➔ Das Recht auf Anbieterwechsel und Datenportabilität muss für die Nutzenden gewährleistet bleiben.
- ➔ Anbieter müssen gängige und offen standardisierte Formate und Schnittstellen nutzen, um einen Anbieterwechsel und Datenportabilität jederzeit zu gewährleisten.

3. Cloud-Souveränität mit Open Source

Das mit dem CADA geschaffene „Cloud computing sovereignty framework“ ist ein wichtiger Schritt zur Verringerung technologischer Abhängigkeiten, insbesondere bei kritischen Infrastrukturen. Wir begrüßen, dass das Framework Aspekte der Kontrolle und extraterritoriale Einflüsse berücksichtigt. Die letzten Monate und Jahre haben gezeigt, dass übermäßige Abhängigkeiten Angriffsflächen geschaffen haben, die Drittstaaten explizit ausnutzen, um wirtschaftlichen und politischen Druck auf Europa auszuüben.

Die im Framework festgelegten Sicherheitsniveaus („Union Assurance Levels“) dürfen jedoch nicht zu unverhältnismäßigen Anforderungen an Anbieter von Open-Source-Produkten und -Dienstleistungen führen.

Änderungsvorschläge:

- ➔ Die in Art. 16 (2) vorgesehene Befugnisübertragung an die Kommission zur Änderung der Sicherheitsniveaus der Union ist sehr weit gefasst, was zu rechtlicher Unsicherheit insbesondere für Anbieter innovativer Technologien und Dienstleistungen führt.
- ➔ Die in Annexes II und III festgelegten Sicherheitsniveaus sind wesentlicher Bestandteil des CADA und sollten daher nicht durch die Nutzung einer Befugnisübertragung herabgesetzt werden können.
- ➔ Die zunehmende Verwendung von Frontier-KI-Systemen für Schwachstellenscans und die Behebung von Sicherheitslücken birgt das erhebliche Risiko einer regulatorischen Schieflage: Wenn die Definition von State-of-the-Art-Cybersicherheit de facto die Nutzung proprietärer KI-Tools und Cloud-Infrastrukturen aus Drittländern voraussetzt, konterkariert dies das übergeordnete Ziel der europäischen Technologiesouveränität. Proprietäre Black-Box-Lösungen bieten keine nachprüfbare Sicherheit, sondern etablieren neue systemische Abhängigkeiten und Kontrollverluste. Wir fordern die Europäische Kommission daher auf, in Annex II, Anforderung 1.1(e) folgende Klarstellungen vorzunehmen:

  1. Technologieneutralität und Souveränität: Die Konformität mit Sicherheitsanforderungen darf Unternehmen und Behörden nicht in proprietäre Vendor-Lock-ins oder außereuropäische Infrastrukturabhängigkeiten zwingen.
  2. Vorrang für Open Source undAuditierbarkeit: Verifizierbare Sicherheit setzt Transparenz voraus. Die Nutzung und Weiterentwicklung von Open-Source-Sicherheitsmodellen (überprüfbarer Quellcode, Open Weights, prüfbare Trainingsdaten, offene Schnittstellen) muss als gleichwertiger oder vorrangiger Pfad zur Erfüllung der Sorgfaltspflichten anerkannt werden.

- ➔ Bei proprietären Schwachstellen-Scannern aus Drittstaaten besteht das reale Risiko, dass Sicherheitslücken aufgrund ausländischer Rechtsvorgaben (z. B. Geheimhaltungspflichten oder staatlicher Zugriffsrechte) gegenüber europäischen Betreibern bewusst verschwiegen oder gefiltert werden. Setzen Anbieter mit Union Assurance Level 1 (UAL1) solche intransparenten Werkzeuge ein, wird das Vertrauensniveau der gesamten Zertifizierung untergraben. Die EU-Kommission muss daher – insbesondere im Rahmen von Annex II,

1.1(g) – verbindliche Leitlinien zur Unabhängigkeit, Auditierbarkeit und Integrität der eingesetzten Sicherheitswerkzeuge vorgeben.

➔ Anbieter müssen gängige und offen standardisierte Formate und Schnittstellen nutzen, um dies zu ermöglichen.

4. „Union added value“ in der öffentlichen Beschaffung

Bei der öffentlichen Auftragsvergabe sollte **Open Source Vorrang vor anderen Auswahlkriterien** haben.

Die Art und Weise, wie Open-Source-Projekte entwickelt und mitgestaltet werden, kann sich erheblich von proprietären Entwicklungsmodellen unterscheiden. Insbesondere aufgrund der Freiheiten, die Open-Source-Lizenzen gewähren, können nicht im gleichen Maße wie bei proprietärer Software Abhängigkeiten entstehen, denn die Nutzenden und Entwickelnden haben jederzeit die Möglichkeit, einen Fork (also eine vom ursprünglichen Hersteller unabhängige Weiterentwicklung der Software) vorzunehmen.

Die aktualisierte Open-Source-Strategie der EU-Kommission schafft ein „Open Source Maintenance Instrument“, das speziell darauf abzielt, die Möglichkeiten für einen Fork zu schaffen, um übermäßige Kontrolle oder Beeinflussung eines einzelnen Herstellers zu vermeiden.

Bei der öffentlichen Beschaffung von Open Source Software müssen den Beschaffern die Mittel an die Hand gegeben werden, um zu bewerten, ob ein Anbieter Verbesserungen und Anpassungen an der Software auch wieder in das Open-Source-Ökosystem zurückfließen lässt. Dabei sollte der **Upstream-First-Ansatz** berücksichtigt werden: Weiterentwicklungen und Verbesserungen sollten möglichst direkt in die ursprünglichen Open-Source-Projekte eingebracht werden, statt dauerhaft getrennte Entwicklungszweige zu schaffen. Dies stärkt die gemeinsame Weiterentwicklung, reduziert langfristige Wartungsaufwände und trägt zur Nachhaltigkeit des Open-Source-Ökosystems bei.

Wenn die Beschaffer entsprechende Bewertungskriterien an die Hand bekommen, können so Anbieter ausgewählt werden, die zuverlässig die langfristige Qualität und Sicherheit einer Software sicherstellen. Anbieter, welche zulasten von Qualität und Sicherheit Preisdumping betreiben, können so ausgeschlossen werden. Die Beschaffer müssen

dementsprechend die Möglichkeit bekommen, bei der Auswahl und Vergabe der Qualität Vorrang vor dem Preis einzuräumen.

Änderungsvorschläge:

- ➔ Art. 32(2)(d) macht nicht-preisbezogene Vergabekriterien zu nachrangigen Auswahlkriterien, die bei der Vergabe des Auftrags nicht ausschlaggebend sind. Diese Regelung birgt die Gefahr, dass alle nicht preisbezogenen Kriterien an Bedeutung verlieren und sollte daher gestrichen werden.
- ➔ Bei der Beurteilung, ob ein Anbieter zur Stärkung der Lieferkette für digitale Technologien in der EU beiträgt, sollte in Art. 32(3)(a) klargestellt werden, dass Beiträge zur Entwicklung von Open Source Software, Hardware oder anderen Technologieprojekten als Beitrag zur Stärkung der Lieferkette der EU anzusehen sind.
- ➔ Das Ziel von Art. 32(3)(b), die Lücke zwischen öffentlich geförderter Forschung und tatsächlichem Markterfolg in Europa (F&E-zu-Markt-Transfer) zu schließen, ist industriepolitisch ausdrücklich zu begrüßen. Eine rein geografische Auslegung birgt im Softwarebereich jedoch die Gefahr systemischer Fehlanreize: Moderne Softwareentwicklung und insbesondere Open-Source-Ökosysteme sind ihrem Wesen nach global und kollaborativ. Dass Open-Source-Projekte Beiträge internationaler Maintainer integrieren oder von globalen Stiftungen verwaltet werden, begründet im Gegensatz zu proprietärer Drittstaaten-Software keine einseitige Kontroll- oder Abhängigkeitsbeziehung. Durch die uneingeschränkte Auditierbarkeit, die freie Weiternutzung und das Recht zur Abspaltung (Forks) bleibt die digitale Souveränität der EU gewahrt. Art. 32(3)(b) muss daher klarstellen, dass global gepflegte Open-Source-Komponenten, die in europäische Wertschöpfungsketten eingebunden sind, die Kriterien für den europäischen Mehrwert vollumfänglich erfüllen und nicht als fremdbestimmte Abhängigkeit gewertet werden.
- ➔ Es sollten spezifische Bewertungskriterien insbesondere für die Beschaffung von Open Source Software hinzugefügt werden: Wenn ein Anbieter sich bereits an der Entwicklung einer Open-Source-Lösung beteiligt hat oder besondere Erfahrung mit der jeweiligen Open-Source-Lieferkette einer beschafften Lösung besitzt, sollte dies in Art. 32 als Auswahlkriterien verankert werden. Dabei sollten

insbesondere Beiträge zur Weiterentwicklung der ursprünglichen Open-Source-Projekte im Sinne des Upstream-First-Prinzips sowie die Beteiligung an deren langfristiger Pflege, Governance und Community-Arbeit positiv berücksichtigt werden.

Wir verweisen an dieser Stelle auch auf unsere Stellungnahme zum EU Public Procurement Act sowie auf die Stellungnahme zum EU Public Procurement Act von APELL, dem Dachverband der europäischen Open-Source-Unternehmensverbände.

5. Zentrale Beschaffung muss technologische Souveränität sicherstellen

Die EU-Kommission hat die Möglichkeit, Beschaffungsmaßnahmen für Rechenzentrumsangebote, Cloud-Computing-Services, Software und KI-Systeme nicht nur für sich selbst, sondern auch für andere EU-Einrichtungen durchzuführen und als zentrale Beschaffungsstelle auch für die Mitgliedstaaten zu fungieren. Wenn die EU-Kommission in dieser Funktion tätig wird oder die Beschaffungstätigkeiten anderer Einrichtungen unterstützt, muss die sie sicherstellen, dass hierbei die Ziele der technologischen Souveränität verfolgt werden.

Änderungsvorschläge:

- ➔ Jede Beschaffungsmaßnahme muss eine Bewertung der Ziele zur Stärkung der technologischen Souveränität beinhalten, insbesondere mit Blick auf die Verringerung von Abhängigkeiten und die Steigerung des „Union added value“. Hierbei müssen auch die Auswirkungen möglicher Fusionen und Übernahmen berücksichtigt werden, insbesondere durch Unternehmen und Organisationen, die außerhalb der EU gegründet wurden oder von außerhalb der EU kontrolliert werden.
- ➔ Jede Beschaffung von proprietären Produkten oder Dienstleistungen muss ausführlich anhand von spezifischen, messbaren und relevanten Kriterien gerechtfertigt werden, die in Title IV, Chapter IV aufzunehmen sind.
- ➔ Wenn die User Experience oder das User Interface Kriterien bei der Auswahl und Vergabe sind, sollten Ausschreibungen eine Möglichkeit vorsehen, dass Anbieter diese Aspekte in einem vorgegebenen Zeitrahmen unter Einbeziehung der Nutzer verbessern dürfen.

➔ Die Laufzeit von Verträgen über proprietäre Produkte und Dienstleistungen muss auf maximal drei Jahre festgelegt werden. Danach muss der Auftrag erneut ausgeschrieben werden und die Ziele zur Stärkung der technologischen Souveränität müssen erneut bewertet werden.

6. Open Source First

Wir begrüßen die Einführung des Open-Source-Kapitels (Title IV, Chapter V) im CADA. Die Regelungen in diesem Kapitel müssen jedoch präzisiert werden um umsetzbar zu sein und Wirkung zu entfalten.

Änderungsvorschläge:

➔ Der derzeitige Wortlaut von Art. 41 wird dem erklärten Ziel aus dem Titel des Open-Source-Kapitels („Open Source first“) nicht gerecht. Anstatt die Verwendung von offenen Standards und Komponenten unter Open-Source-Lizenzen lediglich anzuregen („encourage“), sollte Art. 41 so geändert werden, dass die Verwendung von Open-Source-Lösungen klar priorisiert wird. Es müssen konkrete Verpflichtungen zur Beschaffung von Open Source festgelegt werden und mögliche Ausnahmen müssen klar abgegrenzt und begründungspflichtig sein.

➔ Art. 42 sollte über die Bereitstellung bestehender Software hinaus auch Neuentwicklungen, Anpassungen oder Individualsoftware umfassen, sofern dem keine anderen rechtlichen Anforderungen entgegen stehen.

➔ Der bestehende EU-Open-Source-Katalog, der nun in Art. 43 fest verankert wird, enthält derzeit lediglich Lösungen, die bereits von Organisationen des öffentlichen Sektors genutzt werden. Der Katalog sollte jedoch dadurch einen Mehrwert schaffen, indem er für Einrichtungen des öffentlichen Sektors Informationen über neue Lösungen und weitere Möglichkeiten bereitstellt. Darüber hinaus bietet Art. 43 die Möglichkeit, ein „Open Source Maintenance Instrument“ zu schaffen, wie dies auch in in Abschnitt 4.2 ("Strengthening and promoting a vibrant open source ecosystem") der aktualisierten Open-Source-Strategie der EU-Kommission verankert ist.

➔ „Open Source Programme Offices“ (OSPOs) können ein strategischer Treiber für digitale Souveränität sein, wenn sie auf EU-Ebene

koordiniert werden. Die OSPOs sollten einen strukturierten Dialog mit den Akteuren des Open-Source-Ökosystems etablieren. Die OSPOs können im Rahmen von Beschaffungsverfahren eine wichtige Rolle als „trusted advisor“ innerhalb der öffentlichen Verwaltung spielen und Hinweise und Unterstützung bei der Beschaffung von Open Source anbieten. Das in Art. 44 eingerichtete OSPO-Netzwerk sollte entsprechend finanziell und personell ausreichend ausgestattet werden, damit es sein volles Potenzial entfalten kann.

APELL recommendations for amendments

(accompanying the APELL Policy Brief September 2026 – Cloud and AI Development Act for Digital Sovereignty https://apell.info/wp-content/uploads/2026/09/2026-09_APELL%20Policy%20Brief_CADA.pdf)

Reducing dependencies

Open cloud computing stacks and *open-source middleware platforms* are explicitly mentioned in operational objective 2 (Art. 3(1), 3(2)(b), 4(2)), but **should be the default** also in the *development and deployment of data centre technologies* (objective 1, 3(2)(a)), as well as where *frontier AI capabilities are being developed* under CADA and other instruments.	
Art. 3(2)(a)	(a) supporting the development and deployment of ***open cloud computing stack technologies and*** advanced data centre technologies incorporating principles of energy efficiency and resource efficiency by design and throughout operations (operational objective 1);
Art. 3(2)(c)	(c) advancing Union's capabilities in frontier AI ***supporting the Union's technological autonomy*** (operational objective 3);
Art. 4(3)	Under operational objective 3, the Cloud and AI Leadership Initiatives shall support pioneering projects in frontier AI that develop ***open*** frontier AI models and systems as strategic assets, ***supporting the Union's technological autonomy*** including in key sectors such as cybersecurity.

Article 6 on the *implementation of Cloud and AI Leadership Initiatives* and Article 7 on the *national cloud and AI strategies* should **clearly reflect that operational objectives from Art. 3 must be reflected in implementations at all levels, in particular openness objectives**.	
Art. 6 (3a new)	***3a new. Member States shall report to the Commission on their overall progress of Cloud and AI Leadership Initiatives' implementation at least yearly. The Commission shall monitor the progress in particular of the implementation of the operational objectives.***
Art. 6 (4)	4. To reflect technological and market developments***, or where necessary to contribute to the implementation of the operational objectives,*** the Commission is empowered to adopt delegated acts in accordance with Article 45 to amend Annex I in a manner consistent with the objectives of the Cloud and AI Leadership Initiatives set out in Article 4.
Art. 7(1)	1. By [same day as entry into force plus one year], Member States shall establish national cloud and AI strategies (the 'national strategies') ***pursuing the operational objectives laid down in Articles 3 and 4***.
Art. 7(2)(a)	(a) key objectives and priorities for cloud and AI adoption, in line with the 'AI first' principle***, the operational objectives, and supporting the Union's technological autonomy***, as well as a governance and monitoring framework to achieve those objectives and priorities;

Data centre acceleration without lock-in

Operators should receive priority that build on **open cloud stacks** that make the best effort to not only avoid proprietary components at all levels of the stack. **Priority must be given to Open Source technologies.**	
Art. 14(1)(b)	(b) the project includes highly sustainable***, open,*** or innovative features, including technologies and solutions developed under Title II;
Art. 14(2)	In its proposal, the applicant shall provide all the necessary and relevant information to demonstrate that the project fulfils the relevant criteria ***pursuant to paragraph 1, and operators fully comply with switching and portability rights laid down in Regulation (EU) 2023/2854 (Data Act), making use of commonly used, and openly standardised formats and interfaces***.

Users must **retain their switching and portability rights.** Providers must **make use of commonly used, and openly standardised formats and interfaces** to enable this.	
Art. 14(1)(ea new)	***(ea new) the project gives priority to open cloud computing stacks on the basis of open-source software and hardware, supporting the Union's technological autonomy.***

Open cloud sovereignty

The delegation of power to the Commission in Article 16(2) to **amend the Union assurance levels** is very broad, causing **legal uncertainty** in particular for innovative technology and service providers. As an **essential element of the Regulation**, the assurance levels established in Annexes II and III should not be lowered using a delegated power.	
Art. 16(2)	The Commission is empowered to adopt delegated acts in accordance with Article 45 to amend the Union assurance levels set out in Annex II***, for the purpose of clarifying or rectifying, but not objectively lowering, criteria,*** and the evidence set out in Annex III.

The growing **importance of automated vulnerability scanning** and eventually fixing, in particular relying on frontier AI models, could lead to a situation where *state-of-the-art cybersecurity standards* **could create a requirement to rely on such proprietary, third country-provided, and not technologically sovereign tools/services and infrastructure**. The Commission should clarify this in particular with regard to requirement 1.1(e) in Annex II, but also with regard to other laws and policies.
Similarly, even the *mere use* **of such automated vulnerability scanning** tools/services and

infrastructure by UAL1 qualified providers **could mean exploitable security vulnerabilities exist that are not reported** by the tool/service because of control or legal requirements by a third country. The Commission **should provide guidance** with regard to the integrity of the requirements in particular of UAL1. (in particular Annex II, 1.1(g)).

Union added value in procurement

Art. 32(2)(d) makes *non-price award criteria* ancillary and not decisive in the award of the contract. The provision **risks making all non-price criteria irrelevant and should be deleted**.

Art. 32(2)(d)	***(deleted)***

When evaluating whether a *tenderer contributes to strengthening the digital technology supply chain in the Union*, it should be clarified in Art. 32(3)(a) that **contributions to the development of Open Source** software, hardware, or other technology projects **can be considered as contributing to** *strengthening the Union supply chain* **independently of whether a project is hosted, or contributed to, by entities or individuals in third-countries.**

Art. 32(3)(a)	(a) the tenderer contributes to strengthening the digital technology supply chain in the Union, including ***contributing features, funding, and security fixes to the development of the supply chain of digital technologies that are components to the present solution under open-source licences, or*** the use of software or hardware designed or manufactured in the Union;

Similarly, in Art. 32(3)(b), it needs to be reflected that, while Open Source projects may receive contributions from third countries, or even be hosted by third country organisations, this **does not create the same level of control or dependency** as with non-Open Source technologies.

Art. 32(3)(b)	(b) the tenderer has integrated technologies developed ***under an open-source licence, or developed*** in the Union, including research and development results stemming from Union funded research and development programmes and makes use of tools, such as standards, specification, software, models or other technology developed in the Union;

Add evaluation criteria for tenderers that support the Union’s technological autonomy by guaranteeing freedoms that avoid vendor lock-in and anti-competitive bundling practices, including enabling switching, portability, and interoperability, as well as maintenance, modification, and auditing by way of source code transparency and permissive licencing. **Furthermore add criteria** specifically where Open Source is being procured to evaluate a tenderer's contribution to, familiarity and experience with the specific Open Source supply chain of a procured solution, to **ensure tenderers are selected that contribute to the long-term sustainability and maintenance of the Open Source supply chain**. These should be made actionable as **effective selection criteria** in Article 32.

Art. 32(3)(ba new)	***(ba new) the tenderer supports the Union's technological autonomy by ensuring the supply chain of technologies that are components to the present solution is interoperable, and enables switching and portability, on the basis of commonly used, openly standardised formats and interfaces, and the present solution enables and permits maintenance, modification, and auditing by way of transparent, available, of source code, including for the purpose of discovering and fixing security vulnerabilities, backdoors, improvements, and further re-use and sharing of the solution beyond the foreseen application independent of the present tenderer;***
Art. 32(3)(bb new)	***(bb new) the tenderer contributes to, and has familiarity and experience with, the supply chain of technologies that are components to the present solution;***

See also APELL's response to the publication of the Public Procurement Act and European Innovation Act proposals ("Put Open Source front and centre: Public Procurement Act and European Innovation Act proposals": https://apell.info/2026/09/16/public-procurement-act/), and to the Commission's prior consultations on the procurement revision ("Public Procurement revision: shift investments to Open Source": https://apell.info/2026/01/26/procurement-shift-investments/, and "APELL submission to the Public procurement directives evaluation": https://apell.info/2025/02/20/apell-submission-public-procurement-directives-evaluation/).

Central purchasing must ensure technological sovereignty

Any procurement activity must include an **assessment of the technological sovereignty goals**, in particular reduction of dependencies and increase of Union added value, taking into account the **effect of possible mergers and acquisitions in particular by economic entities established, or controlled by entities outside of the EU**.

Any **procurement of proprietary products or services** must be thoroughly justified along a **fixed set of specific, measurable, achievable, and relevant criteria** to be added to Title IV, Chapter IV.

Where the user experience or user interface are criteria in selection and awarding, tenders should allow for time-bound improvements involving the users.

Art. 34(3)(a)	(a) a catalogue providing information on available public sector data centre services and cloud computing services***, and in particular where open-source solutions or components are being used supporting the Union's technological autonomy***;
Art. 37(1a new)	***1a new. Any procurement activity carried out by the Commission shall include an assessment of the Union's technological sovereignty objectives, in particular the support for the Union's technological autonomy of a service, software or system to be procure, the added value for the Union, taking into account the effects of possible mergers and acquisitions in particular by entities established, or controlled by entities, outside of the EU. Where services, software, or systems not made available under open-source licences are procured, the Commission shall thoroughly justify such procurement along the following exclusive set of criteria:*** ***(i) with the exception of user experience or user interface functions, no functionally adequate alternative or comparable service,***

	software, or system made available under open-source licences exists, and such absence is not the result of an artificial narrowing down of the parameters of the procurement procedure; ***(ii) where no adequate alternative or comparable service, software, or system made available under open-source licences exists that satisfies the criteria in terms of user experience or user interface, exists, a time-bound improvement involving the users is not reasonable;***.

The **performance of contracts** for proprietary products and services must be fixed to a **maximum of 3 years**, after which the contract must be opened for tenders again, and the technological sovereignty goals re-assessed.	
Art. 30(4)	By derogation from paragraphs 2 or 3, on an exceptional basis and where duly justified, contracting authorities may decide ~~not~~ to ***postpone the*** procure***ment of*** cloud computing services recognised as having a Union assurance level 1, 2, 3, or 4 ***by a maximum of two years after [date of entry into force plus 1 year],*** where one or more of the following circumstances applies:
Art. 34(3)(a)	(a) a catalogue providing information on available public sector data centre services and cloud computing services***, and in particular where open-source solutions or components are being used supporting the Union's technological autonomy***;
Art. 34(3)(b)	(b) a service platform for the exchange and orchestration of computing, storage and network resources and services***, and the re-use and deployment of open-source solutions and components supporting the Union's technological autonomy***;

Open Source first

Rather than only encouraging the use of open standards and components under Open Source licence, Art. 41 should be **modified to effectively prioritise their use**. **A derogation from the provision** can be introduced to allow a temporary derogation if necessary and justified, to use non-Open Source components.	
Art. 41	***1.*** The Union and Member States shall take the necessary measures ***for*** Union entities and public sector bodies to ***prioritise the*** use ***of*** and facilitate the reuse of open standards and components released under an open source licence when building their cloud and AI ecosystem or stack, taking into account ***requirements from Union and Member State law, and*** functionalities, including security, total cost, and other relevant, duly justified ~~objective criteria~~ ***functionality requirements***. ***2 new. By derogation to paragraph (1), where Union entities and public sector bodies have exhaustively assessed the requirements of the cloud and AI ecosystem or stack and duly justified requirements exist that cannot be fulfilled using or reusing available and state-of-the-art open standards and***

	components made available under open-source licences, Union entities and public sector bodies may deviate from paragraph 1 and use alternative solutions, for a limited time of 3 years, renewable once or until open standards or components made available under open-source licences become available.

Beyond making available existing software, Article 42 **should also encompass new developments** of modifications or custom software, insofar as no conflicting legal requirements exist.	
Art. 42	***1.*** When making software to which they hold intellectual property rights available for reuse under an open source licence, a Union entity or public sector body shall do so using a catalogue or repository that is connected to, and made accessible through, the EU OSS Catalogue referred to in Article 43. ***2 new. Where the development of modifications to existing software is commissioned, or new custom software procured, it should be released under a recognised open source licence to facilitate its reuse, unless prohibited by Union or Member State law.***

The existing EU Open Source catalogue now codified in Article 43 currently only contains **solutions already in use** by public sector organisations but **should create added value by providing public sector institutions information on opportunities and new solutions**. Furthermore, the Article holds the **opportunity to follow through on the creation of an Open Source Maintenance Instrument** as proposed in part 4.2 ("Strengthening and promoting a vibrant open source ecosystem") of the updated Commission Open Source Strategy.	
Art. 43(1)	The Commission shall provide and maintain an EU Open Source Solutions Catalogue ('EU OSS Catalogue') as a centralised catalogue to access software made available for reuse by Union entities and public sector bodies***, and made available by qualified solution providers***.
Art. 43(3a new)	***3a new. The providers of open-source services, software, and systems shall be allowed to submit their products and services to the Commission or relevant Union entities or public sector bodies for inclusion in the catalogue. Unless rejected on the basis of objective and relevant criteria, including the experience and maintained contributions to the relevant open-source supply chain ecosystem, or lack thereof, submissions shall be published in the EU OSS Catalogue, and solution providers be considered qualified.***

Open Source Programme Offices can be a strategic driver when coordinated at EU level. The OSPO Network established in Article 44 **should receive funding and staff to enable its full potential**.	
Art. 44(1)	The Commission shall establish a network of Open Source Programme Offices ('OSPO Network') to facilitate cooperation on the implementation of the obligations under this Chapter. ***The OSPO Network shall have a***

	secretariat to support its day-to-day tasks.