Berlin/Brussels, 11 November 2026

Statement of the German AI Association on the:

Cloud and AI Development Act[1]

Executive Summary

Europe needs competitive AI companies that can develop and finance their technology and reach customers as urgently as compute and sovereign cloud providers. CADA should strengthen independent European supply while making compute and advanced AI accessible to European startups and SMEs and to the users they serve. Infrastructure investment and effective control must work together with market demand. A framework that expands data-centre capacity without improving access or supplier diversity would deliver too little for Europe's AI economy.

The **German AI Association / KI Bundesverband (KIBV)** supports stronger European capabilities and proportionate protection of critical public functions. Origin and ownership matter and so does effective control. Their consequences should depend on the service and its risk and on the purpose of public support. International capital and technology partnerships must remain possible where European companies retain the control needed for the activity concerned.

I. Assess the service and reuse the evidence: An AI application provider should demonstrate its own contribution and material dependencies, using valid upstream evidence for the underlying infrastructure. Recognition must be usable across borders and procurement procedures.

II. Make independence achievable: Address decisive influence and critical operational dependencies, including exit arrangements that do not work in practice. Avoid fixed foreign-investment caps and universal source-code requirements, and do not promise unlimited technological autonomy. Core systems of police and justice should run at

[1] Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act), COM(2026) 502 final, 2026/0138(COD), 3 June 2026.

Union assurance level 3 by default, with migration within 12 months once a recognised European alternative exists.

III. Create a market for European AI: Align CADA with procurement reform and open contracts to smaller providers. Successful pilots need a competitive route to deployment. European solutions must meet functional requirements; resilience and lifecycle costs must count in purchasing decisions. An AI Adoption and Switching Voucher should help SMEs test, deploy and, where appropriate, migrate to competitive European solutions.

IV. Deliver capacity that companies can use: Coordinate permitting and grid access with financing. Attach meaningful access and capability commitments to public support, and prevent subsidised capacity from becoming captive to a small number of platforms. Strategic data centre projects should be led by European-controlled companies, and the majority of publicly funded capacity should serve users in the Union.

Detailed feedback on the proposal

In June 2026, a provider suspended access to two frontier AI models for almost three weeks to comply with United States export controls.[2] AI models were treated like defence goods for the first time. The KIBV responded that the suspension came as no surprise: hospitals and energy suppliers in Europe rely on systems that a decision taken elsewhere can switch off without warning. The KIBV called for a dependency check in public authorities and critical infrastructure and for sovereignty requirements for AI used by the state.

The dependency is structural. Three non-European providers serve more than 70% of the European cloud market, and a large share of European AI runs on their infrastructure.[3] The European offer is still too small to replace it realistically in the short term. A framework that would close the market overnight would therefore hit the European companies it is meant to strengthen. At the same time, leaving things as they are would keep public services and industry exposed to the next suspension.

For the KIBV, sovereignty means having a choice. A public authority or a company should be able to keep working when a provider or a foreign government withdraws a service, and it should find a competitive European alternative when it decides to switch. The Cloud and AI Development Act can deliver both if it protects the functions where an interruption would do the most harm and builds the European supply that makes switching possible. The KIBV supports the proposal with that aim.

This paper sets out where the assurance framework needs to become workable for European providers and where the development side needs binding commitments. Development is the word in the Act's title that matters most to European AI companies. Each section indicates the provisions of the proposal it concerns.

1. Effective control without closing the market (Art. 2(21), Art. 18, Annex II)

1.1 Assess ownership and operational dependence separately

CADA should distinguish the provider's ownership and governance from control over the service it supplies. A European address does not automatically establish independence.

[2] Anthropic, statement on access to Claude Fable 5 and Claude Mythos 5: https://www.anthropic.com/news/fable-mythos-access. Access was suspended on 12 June 2026 and restored on 1 July 2026. KI Bundesverband, press statement on the suspension, June 2026.
[3] COM(2026) 502 final, explanatory memorandum, p. 1: "three non-EU hyperscalers control over 70% of the European cloud market".

Equally, foreign minority investment does not necessarily confer decisive influence. Guidance under Art. 2 and Annex II should distinguish ordinary investment protections from rights that determine strategic decisions, security arrangements, management or the disposal of essential assets.

1.2 Define control in the Regulation and apply it where it matters

Third-country control decides who can reach the upper assurance levels. From level 3 onwards, a provider and its subcontractors must be free of it (Annex II, point 3.1(g)). A fixed shareholding cap would miss the dependencies that matter. Where a sovereign offering depends on licensed non-European technology, the dependency runs through licences and update channels, and a cap does not reach it. The companies a cap would hit hardest are European firms that raised growth capital abroad.

The KIBV's priority is sovereign AI on European infrastructure and the control test must be strict on substance. A provider whose service can be interrupted or accessed from a third country, including through licence terms, should not reach level 3 on the strength of its share register. The KIBV therefore calls on the co-legislators to define control in the operative text, based on decisive influence and to list the rights that establish it: veto rights over strategic decisions, the right to appoint or remove a majority of a governing body, financing conditions that allow an investor to obtain strategic concessions, and long-term commercial arrangements with comparable effect. Where such rights, alone or in combination, give an investor decisive influence over strategic decisions or critical operations, a minority stake confers control. The 5% threshold in Annex III, point 7.1 should remain a disclosure trigger: it identifies the shareholders an auditor must examine and does not establish control. Standard protective provisions in venture financing, such as consent rights over new share issues, do not amount to control and should not cost a European company its eligibility.

Operators of licensed non-European stacks should meet the same standard of substance. Annex II, point 3.1(i)(ii) requires a migration plan for security-relevant third-country components. That plan should be tested, as Annex III, point 9(3) already suggests, and the test should be binding.

The same substantive approach should apply to technology partnerships and joint ventures. Assessment should establish who can access protected data, alter security-relevant updates, withdraw essential rights or interrupt the service. Corporate form alone should neither establish sovereignty nor determine exclusion. For services

requiring European control, contractual assurances must be supported by credible operational capabilities.

1.3 Distinguish replaceable components from critical dependencies

An application using an externally supplied model or database is not in the same position as an operator whose entire platform cannot continue without one foreign licensor. The relevant questions are how essential the dependency is and what influence it creates. Whether continuity or substitution is practical matters just as much. Indirect dependencies capable of materially compromising the service should be covered, even where no direct contract or access to customer content exists.

For AI services, the assessment should distinguish infrastructure from models, and both from the applications built on them. European hosting does not establish control over a model's licence or availability. But ownership of model weights is not a universal proxy for control over an application. Where the required assurance permits it, demonstrated substitution and appropriately protected data flows should be recognised, as should continued operation. Mandatory ownership of all underlying technology would exclude many specialised European developers.

The proposal leaves a gap at this point. Under Recital 10, a cloud computing service includes remote access to an AI system, but the AI system and its underlying model are excluded. The suspension of June 2026 shows the consequence. A user cannot prevent such an interruption through the choice of hosting provider. The KIBV calls on the co-legislators to ensure that the risk assessment under Art. 29 and the criteria in Annex II cover the availability of the model on which a service depends, including whether a third country can order its withdrawal.

1.4 Keep international cooperation workable

The Art. 18 pathway should use transparent criteria and clear procedures, with review arrangements that providers can predict. Recognition of a country should permit an eligible provider to undergo assessment. The service itself still has to be assessed. Art. 18(2) should also cover a third country that never met the criteria, by referring to a country that "does not or no longer" fulfils them. The Schrems I and II judgments show that such a finding can come late.

1.5 Delete the Union citizenship requirement

From level 3 onwards, Annex II requires all personnel involved in the service to be Union citizens (points 3.1(d) and 4.1(d)). European AI companies recruit globally, and under the cumulative criteria a single engineer without Union citizenship in an operations team would cost a provider its recognition. The risk lies in privileged access. The same points already require a national security clearance for staff handling classified information, and that clearance should be the test. The KIBV calls on the co-legislators to delete the citizenship requirement.

2. One assessment that can be used repeatedly (Art. 16–23, Art. 29(3), Annexes II and III)

2.1 Define the scope before asking for evidence

Recognition should identify the service, deployment configuration, region and material dependencies covered. It should not be treated as a blanket endorsement of every product offered by a provider. For application and SaaS providers, the rules should specify which controls they operate themselves and which are supplied upstream. Controls that depend on the customer's configuration should be identified separately. Responsibility should follow the part of the service that each actor can control.

KIBV proposes an enforceable rule that valid evidence is submitted once and reused for the same requirement. A downstream provider should be assessed on its additional controls and integration choices. Auditors should verify whether the upstream evidence covers the actual deployment and remains current; they should not repeat the infrastructure audit merely because a different company supplies the application.

2.2 Separate ongoing review from a complete new audit

Article 20 provides for annual review. We propose that review of an unchanged service focus on whether the evidence remains valid, taking account of material changes and identified concerns. Surveillance audits in ISO certification practice offer a tested model for this. A new full assessment should require a relevant change or reasoned concern. Authorities should rely on accredited audit findings and concentrate their own examination on legal recognition and supervision, and on issues the audit left unresolved.

National competent authorities should approve auditing organisations against harmonised criteria set at Union level, and the central repository should list the

approved auditors. Providers then know in advance who may audit them, and the outcome of a recognition does not depend on the Member State in which the audit was commissioned.

Published assessment expectations and transparent charges should make recognition accessible to smaller providers, supported by proportionate assistance. Level 1 should retain the SME simplification, with a proportionate route for small mid-caps. At higher levels, define an end-to-end timetable that includes application acceptance and limits unjustified pauses. Successive national reassessments should be excluded. Delayed administrative handling should have an escalation route, without deeming an unverified service compliant.

Audit costs decide who enters this market. Under Art. 20(1), a provider pays for the audit before it has won a single contract at the level concerned. That fixed cost weighs far more on a company with 30 employees than on a hyperscaler that spreads it across a global customer base. Without support, the framework would mainly recognise the companies that can already afford it. The KIBV calls for grants that cover a share of the first audit for SMEs and small mid-caps, financed from the programmes behind the Leadership Initiatives.

2.3 Align auditor rotation with the Digital Services Act

Article 20(4)(a)(ii) excludes any auditing organisation that has audited the provider in the previous ten years. The Digital Services Act, whose independence rules are otherwise almost identical, only bars an auditor after more than ten consecutive years with the same provider.[4] Read literally, the CADA wording would require a different auditing organisation for every audit. It also sits uneasily with Art. 20(8), which allows the annual review to be carried out by the same organisation. In a new and small market of qualified auditors this raises cost without adding independence. KIBV proposes aligning Art. 20(4)(a)(ii) with the Digital Services Act.

2.4 Use equivalent evidence for equivalent requirements

Existing cybersecurity evidence should satisfy overlapping technical requirements where its scope and assurance are equivalent. It cannot substitute for distinct questions of ownership and jurisdiction, or of operational control. The certification alternatives

[4] Regulation (EU) 2022/2065 (Digital Services Act), Article 37(3)(a)(ii): no auditing services to the provider “for a period longer than 10 consecutive years”.

already present in Annex II need common interpretation and predictable transition arrangements.[5]

Source-code requirements must not leave European integrators responsible for obtaining rights they cannot compel a supplier to grant. At the relevant assurance levels, allow independently verified alternatives that provide equivalent protection against the identified risk. Component-level evaluations should be reusable. No alternative should be accepted merely because it is cheaper if it leaves a material risk unresolved.

2.5 Reuse technical facts while retaining legal accountability

A common evidence structure should connect CADA with other applicable digital rules. Service descriptions, data flows, access permissions, deployment locations and material dependencies should be recorded in a form that can be referenced by different assessments. Requiring the same architecture to be described again for each instrument creates cost without improving the underlying evidence.

2.6 Provide common baselines with a clear route for exceptions

The Commission and Member States should publish jointly developed reference assessments for common categories of public-sector activity. These should describe the assumptions and relevant assurance requirements, and the circumstances in which further assessment is needed. Buyers should be able to rely on a baseline where their use fits those assumptions, recording only material differences. Baselines should support decisions. They are no certificate for every deployment of a named product.

2.7 Make assurance evidence understandable to customers

A public recognition entry should explain what was assessed, which deployment it covers, the validity of the recognition and material conditions on its use. Customer-facing information should avoid suggesting that recognition of infrastructure automatically covers every model or application running on it. Detailed commercial contracts and sensitive technical evidence should remain available to authorised reviewers through appropriate access arrangements.

[5] European Commission, COM(2026) 502 final, Annexes II and III, 3 June 2026, points 2.1(e), 3.1(e) and 4.1(e), including national schemes and alternative evidence where no relevant scheme exists.

3. Proportionate protection of public functions (Art. 29–30)

3.1 Choose assurance by workload and consequence

The practical value of the assurance framework depends on consistent purchasing decisions. KIBV supports a common workload-based methodology under Art. 29 and 30. Classification should consider the information processed, the consequences of interruption, access and control risks, and the effectiveness of available safeguards. An institution's sensitive role should not automatically place all its websites and administrative tools in the same category as its critical systems.

The KIBV supports this risk-based approach as the rule. Some systems are so central to the state that the outcome of the assessment should be clear in advance. The Commission's methodology under Art. 29(3) should therefore treat Union assurance level 3 as the default for the core operational systems of police and justice, such as case management systems and investigation records. Defence and national security remain the responsibility of the Member States under Art. 4(2) TEU, and they may require level 3 or 4. Outside that core, level 2 remains appropriate where its safeguards address the identified risks. Common use-case guidance should help buyers apply these distinctions and explain departures. Reducing the number of labels alone would not resolve unclear criteria or repeated assessments. Levels 1 and 2 remain open to providers under third-country control. A recognition at these levels should therefore not be marketed as "sovereign", and the term should be reserved for levels 3 and 4.

We propose a concise control and continuity check within the existing process: identify what must be protected; establish who can materially affect access or continued operation; and verify how the service continues or is replaced if a critical dependency fails. The check should organise existing evidence. It should create neither an additional certificate nor a score that offsets mandatory requirements. To anchor this check, Art. 29(2) should list dependency on a single provider and the realistic availability of alternatives as explicit assessment criteria, together with the ability to switch under Regulation (EU) 2023/2854.

3.2 Make transition obligations deliverable

Migration should follow a funded delivery plan, taking account of replacement capacity, integration, data conversion and continuity of public services. Moving a core police or justice system requires a new procurement procedure and parallel operation. The 12 months in Art. 29(6) are demanding, and they are workable if the obligation is tied to an alternative that exists. The KIBV supports the 12-month period and calls for it to apply

once a functionally equivalent service is recognised in the central repository, so that no authority is required to migrate to an offer that does not yet exist. An extension should require documented reasons and enforceable milestones. Urgent threats require faster action. Extensions should be reviewed against progress and must not become a permanent exemption.

Where no suitable offer exists, buyers should document the functional gap and interim safeguards, and set a date for the next market review. A cheaper headline price alone should not justify preserving a critical dependency. Nor should an authority purchase an unsuitable product simply because it is European. Structured market engagement should turn recurring capability gaps into identifiable opportunities for European suppliers.

Derogations under Art. 30(4) should follow the same logic. A contract awarded below the level identified in the risk assessment should be reviewed against the central repository after 12 months at the latest and include a migration plan that takes effect once a recognised alternative exists. It should be published in the central repository together with its justification, and the authority should announce the re-procurement early enough for recognised providers to show that a compliant alternative exists.

Contracts should include proportionate exit arrangements and usable data exports, with clear continuity responsibilities, building on existing switching obligations. Model substitution requires checks of performance and application behaviour as well as data portability. Multi-cloud or parallel operation can help in particular cases, but should not become a universal requirement for every SME or public body.[6]

4. Public procurement that creates European customers (Art. 32–40)

4.1 Align CADA with the Public Procurement Act

CADA and the proposed Public Procurement Act should give buyers a coherent route to purchase cloud and AI. The procurement reform proposes a digital marketplace and reuse of supplier information. CADA recognition should be usable through that architecture, avoiding a separate document trail for the same service.[7]

[6] Regulation (EU) 2023/2854, Chapters VI and VIII, provides the existing legal baseline for switching and interoperability. The AI-specific measures proposed here supplement that baseline.
[7] European Commission, Public Procurement Act proposal, COM(2026) 590 final, 9 September 2026; European Parliament legislative summary, 2026/0265(COD): https://oeil.europarl.europa.eu/oeil/en/document-summary?id=1912822. Alignment measures below are KIBV proposals. The two frameworks do not yet provide them.

The co-legislators should clarify how CADA's sector-specific assurance and Union-added-value rules interact with general procurement provisions on European preference and on security and resilience. Definitions and evidence should be consistent, as should transition arrangements. Buyers should not have to conduct competing sovereignty assessments under different instruments or reward the same contribution repeatedly under differently named criteria.

Article 32 already provides for contract-linked Union-added-value criteria. KIBV calls for practical guidance that turns this into assessable contributions: European development and maintenance relevant to the service, effective control of supported capabilities, continuity arrangements and the ability to change supplier. Criteria should be proportionate to the contract and compatible with applicable international commitments. Group-wide staffing or royalty ratios are a poor substitute for examining what the contract delivers. The KIBV supports strengthening Art. 32(1) so that contracting authorities actively promote contributions to the European cloud and AI ecosystem. Union added value should be assessed once a tender meets the functional, security and total cost requirements of the contract. Below that threshold, no contribution to the European ecosystem can compensate for a performance gap.

4.2 Give smaller providers a realistic route to contracts

Functional lots should be the default where technically and economically feasible, with reasons required for bundling. Cloud infrastructure should not automatically be purchased with models and applications as an indivisible package. Interfaces and responsibility for integration should be specified so that smaller suppliers can compete without accepting liabilities for the entire stack.

Financial-capacity and insurance requirements should match the contract's size and risks, and so should the references demanded. A provider should be able to demonstrate relevant capability through comparable deployments and technical evaluation; lack of a previous public-sector contract should not itself block entry. Frameworks and aggregated purchases need routes for new entrants and specialist providers, so that demand is not locked into the same suppliers for their full duration.

4.3 Reward performance and credible alternatives

Evaluation should include service quality and total lifecycle cost, including integration, maintenance, exit and avoidable dependency. Buyers should be able to select a solution that meets their needs without matching every feature of an incumbent platform.

Explanations for rejecting a suitable European alternative should identify the actual performance or cost issue and be proportionate to the procurement.

Monitor direct SME contract value as well as participation through prime contractors. The Art. 33 SME objective should create commercial opportunities. Reporting activity alone would miss its purpose. Central purchasing and public cloud federation arrangements should be assessed for their effect on supplier diversity and the demand accessible to independent European firms.

4.4 Make joint offers practical for smaller companies

Smaller European providers should be able to combine complementary services in a joint offer without each having to meet the financial and technical requirements for the entire contract. Procurement guidance should explain how bidders can demonstrate combined capability and allocate responsibilities transparently. Where a lead integrator is needed, its role should be explicit, including interface management and service coordination, as well as the handling of incidents affecting more than one supplier.

4.5 Give buyers the capacity to manage modular procurement

Splitting contracts only works if integration is addressed. Public buyers should identify interfaces and acceptance tests before inviting bids, and budget for integration and supplier management. Where a separate integration service is procured, its specifications should permit substitution of components and avoid giving the integrator unjustified control over future supplier choices.

4.6 Connect pilots with a competitive deployment pathway

A pilot should begin with a defined problem, a budget, agreed success criteria and a description of the procurement route available if it succeeds. Criteria should cover the operational outcome, integration effort, continuing costs and the customer's ability to maintain or change the solution. The subsequent award must follow the applicable procedure; success in a pilot is evidence of capability and creates no automatic right to a contract.

5. Adoption support that reaches companies (Art. 4–6)

5.1 Give the Centres for AI a practical delivery role

The Centres for AI should connect technical advice, suitable providers, testing facilities and routes to finance. They should help a company decide whether AI can address a specific business problem and support implementation where it can. Their value should be judged by completed deployments and continued use. The number of introductory events or referrals says little.

5.2 Keep advice independent and delivery commercially open

Advisory functions should disclose conflicts of interest and distinguish neutral assessment from commercial delivery. If a centre or an affiliated organisation also supplies implementation services, selection and referral arrangements should preserve a fair opportunity for independent providers. Public support should make the commercial market more accessible and must leave viable services supplied by European SMEs in place.

5.3 Combine technology with the skills needed to use it

Eligible adoption activities should include proportionate staff training linked to the supported deployment. This may cover operating the system, checking its outputs, managing data access and adapting the relevant work process. Generic training unrelated to implementation should not consume the project budget. Training should improve the user's ability to operate and switch the solution independently, so that the project does not deepen dependence on one vendor.

5.4 Fund adoption and switching through a voucher

The KIBV proposes an AI Adoption and Switching Voucher for SMEs as an action under the Leadership Initiatives (Art. 4 to 6), delivered through the Centres for AI and existing business-support structures. An adoption route would fund a paid proof of concept and its integration. A switching route would fund the conversion of data and interfaces and temporary parallel operation, where the change reduces a documented dependency. Vouchers should support AI solutions whose provider contributes substantive development and value creation in Europe. AI application and model providers should be eligible without a cloud recognition of their own. Where the supported solution includes a cloud computing service covered by the assurance framework, that service should be recognised at the level the programme specifies. The instrument should be

designed in line with State aid rules, for example under the de minimis Regulation, and financed from the programmes behind the Leadership Initiatives. Infrastructure investment creates supply. The voucher gives the Mittelstand a reason and the means to use it.

5.5 Coordinate funding without duplicating applications

Support intensity and project ceilings should be set using evidence from pilot delivery and the applicable funding rules. Funding ceilings should reflect sectoral costs and expected benefits. Time-limited pilots of the scheme should test take-up, supplier diversity, administrative cost and continued use before wider deployment.

6. Capacity and infrastructure accessible to SMEs (Art. 3–15, Annex I)

6.1 Make publicly supported compute usable

Large-scale frontier capability and accessible compute for specialised AI should reinforce each other. European startups developing industrial applications need a route to capacity without assembling a multinational consortium. Training, fine-tuning, evaluation and inference require different resources and commercial terms. Access arrangements should reflect these needs and should not be designed around the largest training runs alone.

Publicly supported capacity should carry enforceable access commitments proportionate to the contribution and purpose of the funding. These should include an accessible allocation for smaller European users, published terms, manageable minimum commitments and the ability to purchase compute without unrelated proprietary services. Reserved capacity that remains unused should be releasable under transparent rules that preserve the access commitment over time.

Where public money funds strategic capability, European control is a fair condition. The KIBV supports requiring the lead applicant of a data centre strategic project under Art. 14 to meet the establishment and control criteria of Union assurance level 4 in Annex II. These criteria exclude third-country control without the exception available at level 3 under Art. 18. Applying them to the lead applicant alone keeps the door open for technology providers and consortium partners from third countries. Minority investment without decisive influence, as defined in the control test proposed in section 1.2, should not disqualify an applicant.

Article 9(3) covers industrial and physical AI as well as public sector projects, but only with a duty to endeavour. The KIBV calls for a firm obligation and for adding projects based on open source. The degree of openness should be assessed against the licence and the transparency actually offered, as set out in section 7.6. Funding should not depend on publishing complete training datasets, which copyright and data protection law often rule out. Industrial and physical AI must stay in the provision. Article 4(5)(b) promises startups and SMEs in industrial sectors access to the computing resources they need, and Art. 9(3) is the provision that delivers it.

6.2 Coordinate permits and grid access around delivery

Acceleration zones should improve the physical conditions for building infrastructure. Their designation should not determine where individual users must send their data. Site planning, electricity supply, connectivity and administrative capacity must be coordinated so that a faster permit leads to usable computing resources.

Each project should have an accountable coordinating contact and a published checklist, with a consolidated timetable covering interdependent approvals. Missing information should be identified early and coherently, with a clear escalation route for delays. Submission of the same information to multiple bodies should be avoided. Streamlining should preserve environmental requirements and address installation-specific approvals, so that delays are not displaced to a later stage. Because the aggregated baseline permit under Art. 13(2) already covers the assessments at zone level, the maximum duration of the remaining procedure in Art. 13(5) should be reduced from 12 to 9 months for data centre operators established in a Member State. The grounds for suspending this deadline should be listed exhaustively and kept narrow. Faster permits only help if the grid connection follows: transmission and distribution system operators should be required to indicate the available connection capacity for a site within a fixed period on request.

Grid allocation should reflect credible project maturity and delivery, with transparent connection information and safeguards against speculative reservation. Connection capacity that a project has not used by the agreed delivery milestones should be released to the next project in line. Readiness should not be measured only by the ability to make large upfront payments. Viable smaller projects and distributed or edge infrastructure should remain able to compete. The rules for acceleration zones should also cover the extension of existing data centres, which can often add capacity faster because the site and the grid connection are already in place. Strategic designation should explain the practical benefits offered and the conditions attached to them.

6.3 Prevent public investment from reinforcing concentration

Allocation of scarce publicly supported sites and connections, and of the capacity built on them, should consider the resulting supplier diversity. Authorities should monitor whether a small number of groups capture most of the benefits and make access conditions effective for independent providers. Existing viable projects outside designated zones should not be unnecessarily disadvantaged.

6.4 Monitor usable resources and unmet demand

Capacity monitoring should distinguish the requirements of different workloads and report what users can actually obtain. Aggregate data-centre capacity is insufficient to assess access to tightly interconnected training clusters or recurring inference services, and it says nothing about distributed industrial deployment. The monitoring framework should remain technologically adaptable, using workload characteristics in place of a fixed list of processor types.

6.5 Select frontier projects on capability and European benefit

The KIBV calls for deleting the requirement in Art. 8(b) that a frontier AI priority project involve at least three Member States, and for opening the provision to any legal entity eligible for Union funding. Projects should be assessed on technological capability and credible execution, and on their benefit for Europe. A strong project from a single Member State should qualify. Cross-border collaboration should be encouraged where it strengthens the project, but an otherwise eligible applicant should not need to create an artificial consortium. Access routes for specialised industrial projects and smaller users should remain distinct and visible.

Designation should be accompanied by a delivery offer setting out available funding, suitable compute, allocation timing and relevant conditions. Funding and resource-allocation processes should use a common project description and coordinated decisions. A team should not win development funding only to discover that the necessary compute is unavailable during the funded period.

6.6 Match public support to the benefit secured

Strategic data-centre status and accelerated administration serve different purposes, and a sovereignty-specific capital grant serves a third. Eligibility and obligations should reflect the benefit actually provided. Beyond the control criterion for the lead applicant, designation should not import every service-assurance requirement into the project

developer. Where public support is intended to secure strategic European capability, enforceable commitments should cover control of the supported assets and continued access, backed by remedies for non-delivery.

The capacity commitment should be defined against the public contribution or an equivalent measurable benefit. It should specify who can access the resources and on what terms. It should also state how the commitment survives changes of ownership or long-term commercial reservations. Where a strategic project receives public funding, the majority of its computing capacity should be reserved for users established in the Union, with a dedicated allocation for startups and SMEs on published terms.

6.7 Secure the financing the objectives assume

The proposal sets out what should be built but leaves open how it will be paid for. The Leadership Initiatives "may be supported" by existing Union programmes (Art. 6(3)) and State aid rules remain unchanged (Recital 89). The financial statement refers to the next multiannual financial framework and the European Competitiveness Fund.

On the one hand, securing the financing before the objectives are set is a legitimate demand. KIBV proposes anchoring the capacity objective in the operative text and requiring the Commission to publish, before national strategies are due under Art. 7, a consolidated overview of the Union funding available for each grand challenge. Article 14 should define the rights attached to strategic project status, which Art. 14(4) presupposes but does not set out. Strict conditions for lead applicants need rights that make the status worth applying for, such as priority in permitting and grid connection. Designation should be decided independently of any funding decision.

7. Industrial innovation, open technology and data (Art. 2(5), Art. 4, Art. 41–44, Annex I)

7.1 Build on European industrial strengths

CADA should support a broad range of AI business models, including specialised models, physical AI, efficient inference and applications embedded in industrial processes. Public programmes should include routes to real deployment in manufacturing, energy, logistics and other sectors with strong European demand. Shared test environments should help smaller developers demonstrate functionality under realistic operating conditions without creating another product-approval layer.

German and European industrial SMEs need deployment close to production and integration with existing machinery. They also need their commercially sensitive information protected. Support should therefore include edge and on-premises solutions where appropriate, alongside large cloud facilities. Efficient models and alternative architectures should compete on demonstrated performance and resource use, without programme criteria implicitly requiring one platform or hardware ecosystem.

7.2 Support maintainable open technology

Open-source software can strengthen substitutability and independent maintenance. Commercial distribution and professional support should not remove the benefits attached to a qualifying open-source licence, and neither should certification. European SMEs should be able to earn revenue from maintaining and integrating open technology, including components originally developed elsewhere.

Public support should cover maintenance and documentation, as well as upstream contributions, where these sustain useful shared infrastructure. Procurement should assess the resulting benefits for the contract alongside quality and support and in relation to total cost. Neither an open licence nor European ownership alone guarantees a service's operational independence. Open-weight models should be assessed against their actual licence rights and maintainability. They should not automatically be treated as fully open-source software.

Publicly funded development should secure appropriate reuse and access rights reflecting the contribution and purpose of the support. It should not automatically require disclosure of all model weights or of commercially sensitive training data, and it should leave an SME's pre-existing intellectual property untouched. Conditions should be established before the grant or procurement, enabling companies to finance and commercialise their own work.

7.3 Keep technology programmes adaptable

CADA should support agentic applications without creating a separate compliance category for every emerging architecture. AI agents are AI systems within the meaning of Regulation (EU) 2024/1689, and the agent-specific wording in Art. 2(5), 3(2)(f) and 4(6) can be removed. The operative provisions should focus on development and deployment capabilities, while funding priorities can evolve with technological progress. Agentic functionality should not be assumed to exist only in frontier systems. Removing

a dedicated label must not remove eligibility for useful applications built with smaller or specialised models.

7.4 Treat data preparation as part of infrastructure

Compute investment will deliver limited value if companies cannot obtain data that is suitable and permitted for their intended use. Public programmes should support the preparation and documentation of datasets and their maintenance over time, including sectoral and multilingual resources. Publishing a file is not the same as making it usable for model development or evaluation.

Funded datasets should provide intelligible information about provenance, permitted uses, restrictions, versioning and known quality limitations. Where the underlying material cannot be openly distributed, access arrangements should make the permitted use clear and practically available. Documentation should assist compliance without suggesting that inclusion in a public catalogue guarantees every subsequent use is lawful.

7.5 Support interoperable components as well as complete models

The public-sector innovation programme should expressly cover reusable components and application layers, and the adaptation of existing models, alongside the development of new models. Search and retrieval modules, document-processing tools, evaluation resources and integration components can deliver substantial value without requiring a new general-purpose model for every administration.

7.6 Make openness informative

For AI models, buyers and funders should distinguish access to weights, licence permissions, documentation of training methods, evaluation materials and the practical ability to maintain or adapt the model. These dimensions should be described accurately. An unqualified open label hides them. Disclosure expectations must respect applicable rights and should not imply that all underlying training material can be republished.

Greater openness can merit support where it enables reuse or independent evaluation, or where it builds European maintenance capability. Partial openness can still provide useful benefits and should not automatically exclude a model from adoption support. The required rights and evidence should depend on the funded purpose and the use

case, with no presumption that openness alone establishes sovereignty or product quality.

8. Legislative priorities and implementation (Art. 16(2), 24, 45)

8.1 Put the core simplification rules in the legislation

The obligation to reuse valid evidence and to scope recognition to the relevant service should be established in the basic act, together with a duty to justify additional information requests. Implementation measures can specify formats and equivalence criteria, and the procedures for review. The essential protection against repeated assessment should not depend entirely on future guidance or the discretion of individual auditors.

8.2 Keep the essential criteria in the basic act

Article 16(2) allows the Commission to amend the assurance levels in Annex II by delegated act for an indeterminate period, with a review at least every 18 months (Art. 16(3)). These criteria decide which providers may serve the public sector, and providers invest in audits and staffing, and sometimes in their corporate structure, on their basis. Under Art. 290 TFEU, delegated acts may only supplement or amend non-essential elements of a legislative act. KIBV proposes setting the core criteria on establishment, control, personnel and data location in the operative text and limiting the delegation to technical updates. This applies in particular to the control test and the personnel criteria discussed in sections 1.2 and 1.5. Any change to Annex II should apply after a transition period, and a recognised service should be assessed against the changed criteria at its next scheduled audit under Art. 20. Providers are then audited against criteria that remain stable between two audits. Serious new security risks may justify earlier action.

8.3 Enforce proportionately and adjust to evidence

Enforcement should distinguish deliberate deception and serious or repeated failures from remediable administrative errors. Authorities should normally offer a reasonable opportunity to correct low-risk shortcomings, retaining prompt action where customers or critical functions face material harm. Any suspension or withdrawal should identify the affected services and support orderly continuity arrangements where appropriate.

The approach to sensitive public procurement and control thresholds, like the approach to public support, should be assessed against the same objective: building competitive European capabilities without excluding viable European innovators.

CADA should be judged by whether European AI companies can build and finance useful services and sell them with greater control over their future. Accessible infrastructure and reusable assurance reinforce each other, and both depend on demand for European innovation. Implementation should turn those commitments into operating capacity and deployable products that find sustained commercial demand.

—

Contact

Daniel Abbou
Managing Director

Alessandro Blank
Head of Public Affairs

Ann-Kathrin Zierau
EU Policy Manager

Contact: politik@ki-verband.de

—

About the German AI Association

The **German AI Association** (Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V.) is Germany's largest industry association for Artificial Intelligence (AI) and represents over 700 innovative SMEs, start-ups and entrepreneurs focusing on the development and application of AI. We support AI entrepreneurs by representing their interests in politics, business and the media.

The goal of the German AI Association and its members is an active, successful and sustainable AI ecosystem in Germany and Europe. After all, we can only compete globally if the brightest minds and visionaries decide to set up businesses, conduct research and teach in the European Union. Our members are committed to ensuring that AI technology is applied in accordance with European and democratic values and that Europe achieves digital sovereignty. To achieve this, the European Union must become an attractive place for entrepreneurs to do business, where their willingness to take risks is valued and their innovative spirit is met with the best conditions.