

POSITION | DIGITAL POLICY | CLOUD AND AI

Cloud and AI Development Act

Evaluation of the European Commission's regulatory proposal.

5 October 2026

Executive Summary

BDI supports the overall direction of the Cloud and AI Development Act (CADA). Europe urgently needs to expand its cloud, AI and data-centre capabilities, reduce critical technological dependencies, and create better conditions for investments and innovations. CADA addresses several of the right priorities, including improved access to computing power, accelerated data-centre deployment, stronger European cloud and AI capabilities and the strategic use of public procurement. The three-pillar approach – research, development and innovation; data centre capacity; and autonomy – recognises that Europe cannot only regulate its way to technological sovereignty. It must simultaneously develop its own capabilities, deploy infrastructure at scale, and create predictable demand for sovereign European alternatives.

Measures to enhance Europe's digital and technological sovereignty must be risk-based, proportionate and compatible with an open and innovative single market. They have to strengthen European capabilities without resulting in technological isolation, nationality-based exclusions or restrictions on access to best in-class solutions from trusted international players. At the same time, for some clearly defined areas of the public sector, exclusive reliance on European suppliers is a sensible approach,

BDI's policy recommendations at a glance:

BDI welcomes the Cloud and AI Leadership Initiatives and the proposed Experience and Acceleration Centres for AI. These measures should be implemented as a focused industrial and innovation programme, aligned with sector-specific needs and existing initiatives, such as AI Factories and AI Gigafactories. They should deliver tangible outcomes for companies, particularly SMEs and small-midcaps, rather than create additional administrative burdens.

Data Centre Acceleration Zones, strategic project status and shorter permitting procedures can help close Europe's computing capacity gap. Their effectiveness will depend on harmonised criteria, predictable grid access, sufficient supply of affordable low-emission electricity, and proportionate sustainability requirements. In particular, waste heat utilisation should be encouraged where technically and economically feasible but should not become a barrier to investment where local infrastructure or suitable off-takers are unavailable.

BDI also welcomes the objective of establishing a single EU-wide applicable Cloud Sovereignty Framework. A common framework can reduce national fragmentation, improve comparability and provide greater legal certainty. The use of the framework must – as proposed by the European Commission – remain limited to public authorities. The Union Assurance Levels must be applied proportionately to the sensitivity of the use case.

Private companies must remain able to select cloud services on the basis of technical, operational and security requirements, supported by their own risk assessment. German Industry is concerned about the underlying implications of Article 31 (3). The provision would allow the Commission to extend sovereignty-related impact assessments and binding cloud requirements to private companies, including entities that are already regulated under NIS2. This possibility must be deleted as regulated industries already assess and mitigate ICT third-party risks under NIS2, DORA and sector-specific legislation. Adding CADA requirements would duplicate existing obligations, increase compliance costs and directly contradict the EU's simplification agenda. Recital 66 recognises that public procurement requirements influence regulated industries and generates market spillovers. Public-sector demand must give European providers the scale required to invest, innovate and offer credible alternatives. Regulatory intervention in commercial decisions of private companies could weaken operational resilience, limit access to innovative services and risk encouraging third countries to introduce similar requirements, disadvantaging companies operating within global networks.

Public procurement should serve as an anchor market for European innovation and resilience but it should remain competitive, technology-neutral and consistent with international commitments. European added value should be understood as “Made with Europe”, rewarding investment in European infrastructure, research, skills and cybersecurity without creating protectionist or nationality-based preferences. Public procurement can strengthen the European ecosystem and a resilient provider landscape, offering opportunities for providers of all sizes, including SMEs.

To deliver on CADA's well-intentioned objectives without creating additional regulatory burdens, restricting technological choice or weakening European competitiveness, BDI recommends the following priority amendments:

- **Clearly define the reach of the UAL:** The framework should be designed and applied in a proportionate manner to the sensitivity of the use case.
- **Delete Article 31 (3) and keep private-sector cloud choice outside CADA:** The Commission should not be empowered to impose additional cloud requirements on private companies through delegated acts. The public-order justification cannot be transferred to private procurement. Existing obligations under NIS2, DORA and sectoral rules are sufficient.
- **Use public procurement as an effective anchor market:** The public sector must give European providers the scale required to invest, innovate and offer credible alternatives. The Union-added-value criteria in Article 32 should carry meaningful weight. Public administration should act as anchor customer for EU cloud offerings.
- **Accelerate investment in European data-centre capacity:** Harmonise acceleration-zone criteria, shorten permitting procedures and ensure predictable grid access, affordable electricity and proportionate sustainability requirements.
- **Simplify recognition and provide planning certainty:** Introduce an EU-wide single passport under Article 17. Extend migration periods to at least 24 months. Limit delegated powers and stabilise the criteria – reviews should take place no more frequently than every 36 months with a minimum 24-month transition period for recognised services.

Table of Content

Title I General Provisions	5
Chapter I – Subject matter and definition	5
Article 2 – Definitions	5
Title II Research, Development and Deployment Activities For the Cloud and AI Ecosystem ...	5
Chapter I – Cloud and AI Leadership Initiatives	5
Article 3 – General objective of the Cloud and AI Leadership Initiatives	5
Article 4 – Operational objectives of the Cloud and AI Leadership Initiatives	5
Article 5 – Experience and Acceleration Centres for AI	6
Article 6 – Implementation of the Cloud and AI Leadership Initiatives	6
Article 7 – National cloud and AI strategies	8
Article 8 – Criteria for frontier AI priority projects	8
Article 9 – Computing support for AI projects	8
Title III Data Centre Capacities	8
Chapter I – Data Centre Acceleration Zones	8
Article 10 – Designation of data centre acceleration zones	8
Article 11 – Conditions within acceleration zones	9
Article 12 – Single information points	9
Article 13 – Facilitating administrative and permit-granting processes	9
Chapter II – Strategic projects	10
Article 14 – Designation of data centre strategic projects	10
Title IV Autonomy	11
Chapter I – Cloud computing sovereignty framework	11
Article 16 – Scope	11
Article 17 – Recognition of cloud computing service providers	12
Article 18 – Associated third countries	12
Article 19 – Conformity self-assessment	13
Article 20 – Independent audit	14
Article 22 – Central repository of cloud computing services	14
Article 23 – Transparency obligations	14
Article 24 – Penalties and compensation	15
Article 25 – National competent authorities	15
Article 26 – Powers of the national competent authorities	15
Article 27 – Mutual assistance	16
Article 28 – Cross-border cooperation	16

Chapter II – Demand-side measures	16
Article 29 – Risk assessments	16
Article 30 – Public procurement	17
Article 31 – Impact assessments.....	17
Article 32 – Union added value	18
Article 33 – Monitoring of procurement of innovation in cloud and AI	18
Chapter III – European public sector cloud federation	18
Article 36 – Fees for the administration of the EuroCloud Federation	18
Chapter IV – Procurement of data centre services, cloud computing services, software and AI systems by the Commission.....	19
Article 37 – Procurement activities of the Commission	19
Chapter V – Open Source	19
Article 41 – Promoting open source solutions and open source first	19
Title V Final Provisions	19
Article 47 – Review	19
Annex II Criteria for Union Assurance Levels	19
Imprint	22

Title I General Provisions

Chapter I – Subject matter and definition

Article 2 – Definitions

For the first time, CADA introduces a standalone definition of the AI agent (Art. 2: an AI system or coordinated set of AI systems acting with a degree of autonomy and using tools). This matches operational reality, where an agent is a coordinated set of systems using tools under a single accountable owner. We appreciate that the proposal entails this definition. The EU co-legislators must ensure terminological consistency with the AI Act, so that the European legal framework does not carry divergent definitions of autonomous AI systems.

Title II Research, Development and Deployment Activities For the Cloud and AI Ecosystem

Chapter I – Cloud and AI Leadership Initiatives

Article 3 – General objective of the Cloud and AI Leadership Initiatives

German industry considers the objectives set out by the CADA to be an essential starting point for increasing Europe's competitiveness and technological resilience. The CADA should be perceived at European and implemented at national level as an industrial and innovation programme to foster European digital sovereignty. Therefore, we welcome the notion to support European cloud infrastructure, advanced data-centre capacity, frontier and industrial AI, and the deployment of European cloud and AI solutions. The explicit focus on technological autonomy, the development of European cloud computing stacks, and the promotion of the uptake of cloud services provided by European companies are aligned with the long-standing objective to reduce strategic dependencies on non-European technologies. We acknowledge that the proposal aims at enabling both cooperation with trusted partners and at the same time setting targeted requirements where public order is at stake. The current cloud ecosystem in Europe is still marked by too much fragmentation and lacks harmonised rules on what sovereignty actually means, and high dependence on non-EU providers. The implementation of CADA should contribute to a more diverse and competitive European cloud system.

To achieve such manifold goals, the European Union and the Member States need to create an economic environment that rewards innovation, attracts private investment, ensures regulatory certainty and supports the large-scale deployment of sovereign cloud and AI solutions across Europe. The Commission's diagnosis is correct: three non-EU hyperscalers account for more than 70% of the European cloud market, while the combined share of European providers has stagnated at around 15%. CADA is an opportunity to reverse this trend while preserving openness for the large majority of workloads and establishing robust European control where public order, data confidentiality and operational continuity require it. At the same time, German industry stresses the need to ensure that the implementation of the Cloud and AI Leadership initiatives remains focused on strengthening Europe's technological sovereignty through genuine European capabilities.

Article 4 – Operational objectives of the Cloud and AI Leadership Initiatives

BDI welcomes the operational objectives set out in Article 4 as these measures can contribute to reducing strategic dependencies, increasing customer choice and strengthening Europe's position in the global cloud and AI market. To maximise their impact, implementation should consider industry-specific use cases and build on Europe's industrial strengths. Strategic sectors should be given particular consideration, including through the development of practical cloud and AI solutions tailored to specific

industrial needs. The focus must now be on rapid commercialisation, deployment at industrial scale and on areas where Europe can build durable competitive advantage.

In this context, Operational Objective 6 and the related Grand Challenge 7 on AI agents platforms are particularly important, as they recognise agentic AI as an infrastructure layer and support the development of sovereign, secure and scalable orchestration frameworks for Europe. Article 4(2) and Grand Challenge 2 should explicitly encompass telco cloud, federated edge-cloud infrastructures, network-compute orchestration and open interfaces. Europe's networks are a strategic asset for low-latency AI, industrial applications and 5G/6G services. The European Edge Continuum and IPCEI-CIS demonstrate the potential of combining connectivity, cloud and edge across providers and borders. Such frameworks can enable the trustworthy deployment of AI agents at scale and should promote transparency, accountability, graduate human oversight and clear governance structures in multi-agent environments. Security and certification requirements should be designed in a proportionate manner. Layered compliance models can help companies consume, develop and provide cloud services without disproportionate audit costs.

Article 5 – Experience and Acceleration Centres for AI

The establishment of the Centres for AI is a practical and viable step. In particular, the strong focus on small medium sized enterprises (SMEs), skills development, technology transfer and the scaling of innovative European companies addresses key barriers that continue to limit the broader uptake of AI across Europe.

At the same time, the effectiveness of the centres will ultimately depend on their ability to deliver tangible outcomes for businesses rather than creating additional administrative structures. German industry therefore encourages a pragmatic and industry-driven implementation that remains closely aligned with regional strengths and market demands. The centres should serve as catalysts for investment, innovation and AI development, actively connecting SMEs, public bodies and industrial users with European cloud and AI providers, providing migration and scaling support, and facilitating access to European compute and data ecosystems. Regional diversity in capabilities and strengths ought to be taken into perspective to nurture a variety of demands.

Particular attention should be given to ensuring complementarity with already existing or at least envisioned European initiatives, such as AI factories and AI Gigafactories, to avoid overlaps, duplication of efforts and fragmented support structures. The centres should focus on the practical deployment and adoption of AI, supporting SMEs, small mid-caps (SMCs) and public sector bodies in translating innovation into market ready applications and scaling AI use cases. By doing so, the centres can be an important piece to complete the overall puzzle of European digital sovereignty.

Article 6 – Implementation of the Cloud and AI Leadership Initiatives

The Cloud and AI Leadership Initiatives have the potential to strengthen Europe's sovereignty while also creating internationally competitive large-scale cloud and AI infrastructure capabilities. A common European approach is essential but must be practical and clearly structured.

It is of great importance to avoid fragmentation and instead strengthen the cohesiveness of the single market. In this regard, the different pillars of the Cloud and AI Development Act should be pursued in a coherent and coordinated manner. Capacity building, deployment objectives and the sovereignty framework are closely intertwined and should not be separated, as doing so could undermine the overall effectiveness and consistency of the initiative. The financing of the Cloud and AI Leadership Initiatives must be secured over the long term to provide a stable and predictable investment environment. State-aid notification, approval and reporting must be significantly faster and simpler. Funding should cover pilots, industrialisation, deployment and procurement – not only early-stage research. The

successful expansion of data centres is an essential precondition for the development and deployment of cloud services, advanced AI systems and emerging AI-agent ecosystems in the Union. There is a risk, that the tripling of data centre capacity may not be achieved within the planned timeframe.

Furthermore, the integration of data centres into local energy planning can contribute to greater energy efficiency while creating benefits for both the operators and local communities. However, a pragmatic approach to energy efficiency requirements is essential, particularly with regard to the utilisation of waste heat. Where technically and economically feasible, the reuse of waste heat should be encouraged and facilitated. At the same time, projects should not be disadvantaged where local conditions, the absence of suitable heat off-takers or other technical constraints make waste heat recovery impractical. The inability to utilise waste heat should therefore not negatively affect the permitting process or the eligibility of a project.

Additionally, ensuring the long-term availability of affordable electricity and accelerated permitting and expansion of electricity networks on all voltage levels will be essential to provide planning certainty for infrastructure investments. Tax incentives for data centre operators could provide further motivation.

Establish a clear legal framework for measures providing support for electricity costs of European providers. The creation of data centre acceleration zones is a step in the right direction. However, the advantages of such acceleration zones can only be utilised if sufficient investments in the development of data centre infrastructures are generated. The creation of data centre acceleration zones will fall short if the CADA fails to sufficiently address the issue of high electricity prices. An investment-friendly location policy is therefore a necessary condition for achieving the sovereignty and resilience objectives pursued under the CADA. Particularly in the data centre sector, electricity prices constitute a significant – if not the central – competitive factor and account for 30–50 per cent of operating costs. High electricity prices compared to international benchmarks are an obstacle to the development of a sovereign and resilient data centre infrastructure.

A clear, stable and predictable framework for grid access is equally essential for long-term planning and investment and for building low-emission, clean-powered data centres. German industry supports the shift from a first-come, first-served to a first-ready, first-served (FRFS) approach to grid connection, as set out in the Commission's Grids Package. Non-binding guidance is, however, insufficient: a set of core criteria and high-level procedural steps should be embedded in EU law to support a coherent and harmonised interpretation of the FRFS principle across Member States, in particular (i) clarity on the evidence required to demonstrate project maturity, so as to reduce the administrative burden on both applicants and system operators, and (ii) principles for a gated, multi-stage approach to progression in the connection queue that provides transparency, predictability and investment certainty.

A clear distinction between the services run by the data centre operators and pure cloud service providers is essential. The legal framework must sufficiently distinguish between the different purposes of data centres, as for example data centres used for upholding connectivity already face regulations regarding security and resilience which may lead to trade-offs with sustainability.

It is necessary to be flexible to respond to technological and unforeseen developments. Therefore, it is paramount that amendments to Annex I are made in a transparent manner and with appropriate stakeholder consultation to provide long-term certainty for investment and industrial planning.

In light of the above stated recommendations, German industry would welcome the implementation of the following amendments to the current draft law:

4. To reflect technological and market developments the Commission *after consulting industry* 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.

Article 7 – National cloud and AI strategies

While German industry supports the requirements for Member States to establish national cloud and AI strategies in general, it deems the proposed period of twelve months to be excessive. Given the rapid nature of technological advancements, delicate geopolitical shifts and the understanding that each Member State already has measures in place, German industry sees a six-month timeframe as appropriate to achieve the objectives more swiftly.

In light of the above stated recommendations, German industry would welcome the implementation of the following amendments to the current draft law:

1. By [same day as entry into force plus ~~one-year~~ *six-months*], Member States shall establish national cloud and AI strategies (the ‘national strategies’).

The national cloud and AI strategies should include clear metrics for connectivity infrastructure, inter-connectivity between data centres with a view to inferencing and Edge AI and especially security and resilience of the Cloud and AI Infrastructure.

Article 8 – Criteria for frontier AI priority projects

German industry welcomes the establishment of a framework for the recognition of frontier AI priority projects to scale up promising projects as quickly as possible. The designation process must remain transparent, efficient and adapt to the fast-changing nature of such undertakings and not force initiatives in a one-size-fits-all structure to secure funding and allow for long term planning.

Article 9 – Computing support for AI projects

BDI embraces that with Article 9 the European Commission ensures strategically important European AI projects to have sufficient access to computing power by combining EU and national resources while stimulating cooperation between Member States.

Title III Data Centre Capacities

While German industry supports the data centre-related proposals enshrined in the CADA in general, to avoid duplication of obligations and concentrate resources as efficiently as possible, coordination of goals and measures between the CADA and the Industrial Accelerator Act and the Data Centre Sustainability Rating Scheme is paramount.

Chapter I – Data Centre Acceleration Zones

Article 10 – Designation of data centre acceleration zones

German industry supports the establishment of data centre acceleration zones in the Member States. The European Union currently lags behind other major regions, such as the United States and China, in both available computing capacity and projected data centre development. Against this backdrop, the Commission rightly identifies the simplification of permitting procedures for the construction,

expansion and modernisation of data centres, as well as the expansion of energy infrastructure, as key levers for accelerating the deployment of data centre capacity across the EU.

We also welcome the inclusion of data centre deployment in acceleration zones within spatial development planning. The designation of suitable sites should become an integral part of local and regional development strategies. This requires close coordination with existing commercial and industrial areas, while taking into account the availability of energy infrastructure capacity, grid connectivity, digital connectivity and latency requirements as well as the potential for waste heat utilisation. Preparing planning procedures for suitable locations has the potential to avoid the lengthy process of establishing zoning and land use plans.

With regard to the criteria set out in Article 10 (1), it is essential to ensure that the objective of accelerated deployment is not undermined by overly restrictive sustainability and efficiency requirements, such as prioritising brownfield sites. Data centre operators have a strong commercial incentive to maximise the efficiency of their facilities. Where facilities operate at lower levels of efficiency, this is often the result of higher redundancy requirements, particularly in data centres providing services for security-critical applications and essential infrastructure. Furthermore, acceleration zones should be solely dedicated to facilitating the deployment of data centre capacity and should not be burdened with unrelated policy objectives. To maximise their effectiveness, Data Centre Acceleration Zones should also be based on clear and transparent criteria for connectivity infrastructure, interconnectivity and the security and resilience of the underlying infrastructure, thereby supporting efficient deployment and enabling the full investment potential of data centre projects. Critically, Article 11(2) should explicitly require Member States to assess concentration across acceleration zones and prevent a single undertaking or group from reserving a disproportionate share of scarce land, grid or connectivity capacity. Allocation mechanisms should reward project readiness, efficient use of resources and provider diversity. Articles 10, 11 and 14 should take account of whether a project expands European-controlled cloud and AI capacity, supports services capable of meeting Union assurance levels 3 or 4, integrates European technologies and provides capacity to public-sector or critical workloads.

Article 11 – Conditions within acceleration zones

As currently drafted, CADA leaves broad discretion to national authorities to define the conditions for access to acceleration zones, which risks divergent criteria across Member States and a race to the laxest threshold. German industry recommends anchoring access to a common EU baseline defined by the EU data-centre rating scheme currently being developed by the Commission. A single EU-level benchmark would ensure that accelerated permitting rewards the highest sustainability performance, strengthen the level playing field and reduce fragmentation and gold-plating across Member States, while giving operators the harmonised, predictable conditions they need to invest.

Article 12 – Single information points

German industry supports the establishment of a single information point for data centre operators. While we acknowledge that the allocation of administrative responsibilities may necessitate the designation of more than one information point in some Member States, the overall objective should be to keep their number to a minimum. Where multiple information points are unavoidable, it must be clear, transparent and straightforward for applicants to determine which information point is responsible for each procedure. Any fragmentation of responsibilities should not undermine the effectiveness of the one-stop-shop approach or create additional administrative burdens for project developers.

Article 13 – Facilitating administrative and permit-granting processes

German industry strongly supports the provision that data centres deployed in acceleration zones shall be considered strategic projects within the meaning of Article 14 of the CADA. Likewise, the

introduction of an aggregated baseline permit is a welcome step towards reducing administrative complexity and increasing planning certainty for investors. The concept of carrying out the necessary planning and environmental assessments at the level of the acceleration zone before individual projects are deployed reflects a pragmatic and forward-looking approach to infrastructure planning. It can significantly shorten project lead times and reduce administrative burdens while maintaining the required level of environmental protection.

Furthermore, the requirement that permit-granting procedures for data centre projects located in acceleration zones should not exceed 12 months, together with the designation of these projects as being of the highest possible national significance where such a status exists in national law, represents an important step towards faster, more predictable and investment-friendly permitting procedures. To ensure that these benefits materialise swiftly, Member States should designate data centre acceleration zones without undue delay.

Both CADA and the Environmental Omnibus under-use the potential of artificial intelligence to speed up administrative decisions. German industry therefore recommends explicitly enabling the use of AI systems, as defined in Regulation (EU) 2024/1689, as a tool to facilitate permit-granting and administrative procedures, in Article 13(5) CADA and in Article 10 of the Environmental Omnibus regulation.

Chapter II – Strategic projects

Article 14 – Designation of data centre strategic projects

Article 14 empowers the Commission to designate certain data centre projects as strategic projects, provided that they meet the criteria set out in the Regulation. As highlighted in our comments on Article 10, the acceleration of permitting procedures is a key prerequisite for expanding data centre capacity in Europe. In this regard, the streamlined environmental assessment procedures foreseen for strategic projects are a welcome measure.

However, BDI believes that eligibility for strategic project status should already be granted where a project fulfils at least one of the criteria listed in Article 14 (1). Requiring projects to meet at least two criteria may unnecessarily limit the number of projects that can benefit from accelerated procedures and thereby reduce the effectiveness of the instrument. Article 14 should include an additional strategic-project criterion covering a project's contribution to a diverse and autonomous European cloud ecosystem. Union and national support should be targeted at additional capacity with demonstrable European added value and should not crowd out private investment or reinforce existing market concentration. European providers and multi-provider projects must have realistic access to acceleration-zone benefits.

In addition, the designation as a strategic project should remain valid for the entire duration of the project. The status should therefore not be linked solely to the initially predicted project lifetime, as project timelines may evolve over time due to operational, regulatory or market-related factors. A strategic project should retain its designation for as long as it continues to fulfil the relevant criteria.

Furthermore, designation as a strategic project under Article 14 should give access not only to Union funding but also to the full permitting simplifications of the Environmental Omnibus, in line with the treatment of strategic projects under comparable Union legislation such as the Industrial Accelerator Act. Otherwise, projects designated precisely to address a major shortage of computing capacity would be denied the very acceleration they are meant to receive.

Title IV Autonomy

Chapter I – Cloud computing sovereignty framework

Article 16 – Scope

German industry welcomes the establishment of a single, EU-wide framework for assessing cloud sovereignty, as it can reduce the fragmentation created by diverging national criteria, such as Germany's BSI C3A or France's SecNumCloud, and improve comparability and legal certainty. Especially, we agree that the proposal should focus on the public sector and public procurement as drivers of demand for sovereign cloud solutions. The private sector cloud procurement should be kept out of scope. We welcome the inclusion of a detailed set of criteria in Annex II of the proposal, which enhances transparency and democratic control. An EU-wide applicable framework reduces costs for cloud service providers as they only have to apply one central framework and thereby increases the profitability and competitiveness of companies operating on the European market, which is in particular crucial for SMEs. We support the approach to mandate the use of the framework by public authorities while keeping the framework in essence voluntary for the private sector. In addition, we welcome the inclusion of a detailed set of criteria in Annex II of the proposal, which enhances transparency and democratic control. An EU-wide applicable framework mirrors industry's call for deepening the digital single market. The framework should be designed and applied in a proportionate manner.

This direction is reinforced by recent political signals. The Franco-German Joint Paper on Digital Sovereignty (17 June 2026) frames sovereignty in expressly risk-based, proportionate and anti-protectionist terms, stressing that strengthening digital sovereignty does not mean turning towards protectionism or isolationism and that Europe should continue to cooperate with trusted international partners while preserving access to state-of-the-art digital solutions. The D9+ declaration from Luxembourg (June 2026) points in the same direction, calling for digital sovereignty to be pursued in an open, pragmatic and interoperable manner that recognises the strategic role of international partnerships. To increase Europe's digital sovereignty while avoiding autarchy, BDI encourages the co-legislators to maintain the ambition level of the sovereignty framework and its binding effect on the public sector.

German industry urges the European co-legislators to create legal certainty through clear definitions. Terms such as "public order", "control", "dependency" "sovereignty" and "union added value" must be clearly defined to avoid fragmentation across single market.

CADA ties higher assurance levels to activities that 'contribute to the preservation of public order'. To ensure legal certainty for all providers bidding into the public sector, the Commission should provide guidance clarifying which types of public sector workloads may typically correspond to which assurance levels. This is necessary to prevent Member States from applying different thresholds when assessing which public sector activities require which assurance levels. The co-legislators must ensure that criteria are objective, transparent and predictably applied: The framework necessarily must differentiate between providers according to the sovereignty characteristics of each assurance level. We welcome that differentiation rests on defined, verifiable criteria that providers can assess against in advance, rather than on discretionary case-by-case judgement. The framework rightly recognises technical, contractual and organisational safeguards. We appreciate that providers that demonstrably meet the criteria of a given level should not be excluded on grounds outside those criteria.

Considering technological developments, reviewing the respective Annexes II and III every 18 months is too short for investment and portfolio planning. Reviews should take place no more frequently than every 36 months, except in a duly justified emergency, with a public report to the European Parliament and Council and a minimum 24-month transition period for recognised services. Such reviews must always entail close industry involvement to ensure that industry's expertise is sufficiently considered.

Moreover, Article 16(2) should permit only technical updates to Annexes II and III, not fundamental changes to the logic or scope of the assurance levels.

German industry also believes that there should be close links with other legal frameworks, in particular the Cyber Resilience Act and the Cyber Security Act, and that duplication of tests and conformity assessment efforts, and double reporting ought to be avoided.

In light of the above stated recommendations, German industry would welcome the implementation of the following amendment to the current draft law:

3. To ensure Annex II and Annex III remain up to date with new legal or technical developments, the Commission shall review them – *based on a thorough consultation of stakeholders from industry and public administration* – at least every 18 months.

Article 17 – Recognition of cloud computing service providers

Article 17 establishes a clear but highly bureaucratic procedure for recognising cloud computing service providers. BDI supports the introduction of an EU-wide single passport under Article 17. A positive third-party audit and recognition by the competent authority of establishment should take effect across the Union. The routine 60-day peer-review period, reasoned-objection procedure and possible Commission arbitration in Article 17(5)-(10) should be removed or confined to exceptional, substantiated cases. The primary responsibility should remain with the Member State of establishment, supported by harmonised methodologies and cross-border cooperation. All national authorities of each Member State should cooperate in the recognition process to ensure that such processes are carried out promptly. Moreover, the Regulation should provide sufficient transition periods and legal certainty to avoid unintended operational risks for existing services.

In light of the above stated recommendations, German industry would welcome the implementation of the following amendment to the current draft law:

17. The competent authority of establishment shall be the evaluating national competent authority. An evaluating national competent authority that has received an application for a candidate recognition, may, where necessary, request one or more competent authorities of the other Member States to collaborate in the procedure for a candidate recognition under this Article. Within 15 days of receiving such a request, the national authority that has received a request for collaboration shall ~~either~~ provide confirmation that it agrees to collaborate with the evaluating national competent authority ~~or refuse the request~~.

Article 18 – Associated third countries

German industry recognises the European Commission's intention to strengthen the EU's digital sovereignty whilst remaining open to trusted third countries and therefore supports the criteria listed in Article 18 paragraph 1 a to f. Stimulating demand for cloud solutions developed in and operated in the EU is paramount. Most importantly, public administration should utilise public procurement as a lever to function as an anchor customer for EU cloud offerings. The higher assurance levels (UAL3 and UAL4) are not merely about 'managing dependencies' but about avoiding disproportionate dependencies and achieving a degree of EU autonomy that is required for high-security use cases. The Commission has carefully analysed that the geographic requirements are WTO-compliant and justified by public order considerations. The co-legislators should strive to increase European digital capacities and capabilities without adopting protectionist measures that block European users from innovative solutions from third countries. To support investment decisions for UAL 1 and UAL 2, the Commission should identify an initial set of selected trusted third countries as quickly as possible.

Despite our general appreciation of the European Commission's goals, the transition towards European cloud sovereignty should reflect market realities. To support the development and uptake of European cloud services, the public sector should perform its role as an anchor customer. The derogations in Article 30(4) must remain exceptional, transparent and narrowly interpreted. Public procurement can and should drive the scaling of European providers while maintaining service continuity for existing critical operations

The framework should recognise technical, contractual and organisational safeguards at the lower assurance levels where appropriate, and avoid designs that exclude providers which demonstrably meet the requirements. Criteria should be objective, transparent, evidence-based and consistent with EU law and international trade commitments. At the higher assurance levels (UAL3 and UAL4), geographic requirements remain appropriate and necessary to preserve public order, as the Commission has carefully analysed that these are WTO-compliant and justified by public order considerations.

Concretely, such safeguards should be recognised as equivalent or complementary pathways to meeting sovereignty requirements, rather than relying on corporate nationality or the geographic origin of hardware. They include technical controls such as client-side encryption, customer-managed encryption keys, confidential computing environments, workload isolation and identity and access management; operational safeguards such as EU-based operational entities, restricted and monitored administrative access, security-cleared personnel and auditable operational procedures; and contractual protections that safeguard customer data against unauthorised access and ensure compliance with EU law. Customer-managed encryption keys should be championed as a concrete, verifiable safeguard and should not be excluded from the sovereignty conversation.

The recognition pathway for trusted third countries described in Article 18 should be transparent, rules-based, timely and non-discriminatory, aligned with existing EU adequacy and trade-equivalence frameworks. The current criteria under Article 18 for designating "trusted third countries" at UAL 3 are overly restrictive.

In particular, the framework should clarify how the criterion of "restrictive measures" that may be imposed by third countries is to be applied. If the mere theoretical possibility of such measures were treated as disqualifying, no non-EU country could ever qualify, as the ability to impose such measures is inherent to the sovereignty of a state under customary international law. The criterion should instead refer to extraordinary, concrete disruptions, together with workable mechanisms for mitigating them. The framework should also avoid being excessively dependent on reviews of individual measures that may give cause of exceptional disruptions, avoiding the pitfall of creating a continuous review of all measures put into place by a third country that would essentially eliminate any legal certainty for companies relying on the associated third countries status. Lastly, the proposal should clarify how the recognition and suspension of the status of associated third country would work in practice, especially, building into the system a cooldown period in case of suspension to allow public sector entities and cloud services providers to adjust to a suspension.

Article 19 – Conformity self-assessment

German industry strongly supports the utilisation of conformity self-assessment by cloud computing service providers aiming at offering their cloud solutions for level one. Conformity self-assessment ensures conformity with regulatory requirements without requiring costly third-party conformity assessment. By making "conformity self-assessment" sufficient for level one, the European Commission adopts the necessary risk-based approach and avoids unnecessary regulatory burden and cost.

Article 20 – Independent audit

Requiring cloud computing service providers offering their services at assurance levels two, three or four to undergo third-party assessments is a viable option and ensures that such offerings are fulfilling the sovereignty and risk requirements necessary for more sensitive or critical use-cases. ISO 27001, BSI C5 and equivalent certifications should be recognised as valid audit evidence to avoid duplicative audits and certification bottlenecks. Article 20 should require audits and opinions to be completed within a defined period – for example, 120 days – with one justified suspension of no more than 30 days. Statutory deadlines for authorities are ineffective if the preceding audit can remain open indefinitely. Furthermore, the CADA should be aligned especially with the AI Act, NIS2, GDPR, CRA and sector-specific requirements to avoid duplications, inconsistencies, and excessive administrative burden.

The CADA proposal should include clarifications on how the backlog of auditing and certification will be managed and absorbed by EU and Member States authorities, to ensure that companies can continue to offer cloud services in the interim, and public sector entities are not frozen out of access to cloud services pending absorption of a high number of requests, especially in the early implementation stages of CADA.

We appreciate that Article 20(8) introduces an annual review requirement since it ensures continued compliance. Nonetheless, the following aspects should be considered:

Article 20 regulates the relationship between provider, auditing organisation, and competent authority – but does not address what information the customer of the recognised service can rely on. Operators required to perform risk assessments under Article 29 need access to at least summary audit attestations to substantiate their own assessments. We recommend that Article 22 (Central Repository) or Article 20 itself require that a summary of the positive audit opinion (scope, UAL level, period covered) be made accessible to customers of the recognised service – not only to competent authorities.

Article 21 provides that auditing organisations shall assess compliance based on audit evidence listed in Annex III. We recommend that the delegated acts under Article 21(1) explicitly recognise existing certification schemes (BSI C5 Type 2, ISO 27001, SOC 2 Type II) as valid audit evidence for overlapping criteria, avoiding redundant audit processes.

The requirement that auditing organisations must not have provided auditing services to the same provider in the 10-year period preceding the audit is extremely restrictive. Given the limited number of qualified cloud auditing organisations in Europe, this risks creating a bottleneck. A 5-year rotation period (aligned with financial audit best practices) would be more proportionate while preserving independence.

Article 22 – Central repository of cloud computing services

Establishing a central repository of cloud computing services at Union level is a very sensible approach since it will provide users of cloud computing services with an overview of available cloud offerings that fulfil the requirements of the four assurance levels. German industry supports the idea to establish a dedicated and easily accessible website to this end.

Article 23 – Transparency obligations

Up-to-date information on cloud computing offerings are paramount to ensure that no cloud computing service provider has an unduly competitive advantage emanating from inaccurate information. However, transparency obligations should remain proportionate and practicable for complex software supply chains. Large operators frequently rely on multi-layer supplier ecosystems including commercial software and open-source components. Additional transparency obligations should therefore be accompanied by clear implementation guidance and realistic compliance timelines.

Article 24 – Penalties and compensation

To ensure that all cloud computing service providers abide by the requirements stated in Articles 16 to 28 the introduction of penalties seems justified. This will contribute to the creation of a level playing field. However, to achieve the aim of harmonisation and fostering the European digital single market, German industry urges the European co-legislators to agree on EU-wide harmonised penalties and compensation mechanisms. The Regulation should not only define penalties but also establish clear transition and remediation mechanisms. Where cloud service providers temporarily fail to meet regulatory requirements, users need legal certainty regarding transition periods, remediation plans and continued operation of existing services.

In light of the above stated recommendations, German industry would welcome the implementation of the following amendment to the current draft law:

1. *The European Commission* ~~Member States~~ shall lay down the rules on penalties applicable to infringements of this Chapter by cloud computing service providers. ~~within their competence and Member States~~ shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. ~~Member States shall, as soon as possible, notify the Commission of those rules and of those measures and shall notify the Commission of any subsequent amendment affecting them.~~
2. *The European Commission* ~~Member States~~ shall take into account the following non-exhaustive criteria for the imposition of penalties for infringements of this Regulation:

Article 25 – National competent authorities

Article 25(4) establishes the “main establishment” principle for exclusive competence. From the perspective of a NIS2 Annex I entity operating across multiple Member States and consuming cloud services from providers established in different jurisdictions, two clarifications are needed:

Coordination with NIS2 authorities. Article 25 does not specify how the competent authority established by the CADA shall coordinate with the competent authority under NIS2 supervising the same operator's risk management. The Regulation should explicitly require cooperation protocols to avoid duplicative or contradictory supervisory demands on operators who are both cloud consumers (under NIS2) and subject to CADA procurement obligations.

Technical expertise requirement. Article 25(3) requires that competent authorities have “sufficient technical, financial and human resources to adequately supervise all cloud computing service providers within their competence.” We welcome this provision but stress that sovereignty assessments require fundamentally different expertise than cybersecurity assessments – including knowledge of extraterritorial legal frameworks, supply chain analysis, and operational continuity. Member States should ensure this expertise is available, not merely assumed.

Article 26 – Powers of the national competent authorities

Article 26(2) grants powerful enforcement tools – including the ability to order cessation of infringements and impose remedies. From an operator's perspective, these powers – particularly the power to revoke a provider's recognition – can have cascading effects on all customers running on that provider.

The Regulation should explicitly require that:

- Enforcement actions that could affect service continuity include an impact assessment on customers and a transition period proportionate to the number of entities relying on the provider.

- Article 26 should cross-reference Article 29(6), which already provides a 12-month migration transition. Any enforcement-triggered loss of recognition should trigger at least the same or longer transition period for affected customers.
- Operators already running workloads on a provider whose recognition is revoked must not be deemed non-compliant with Article 30 during the transition period.

Article 27 – Mutual assistance

Article 27 establishes mutual assistance but frames it primarily in terms of information sharing and investigative support. To reduce implementation costs for operators deploying the same cloud provider across multiple Member States, harmonised implementation is crucial.

Article 28 – Cross-border cooperation

German industry appreciates that national competent authorities are required to closely cooperate with one another to ensure a stringent implementation of the requirements laid down in Annex II of the CADA.

Chapter II – Demand-side measures

Article 29 – Risk assessments

For European public bodies and for pan-European providers alike, predictability is essential for cloud investment decisions and procurement planning. Therefore, German industry supports a mandatory, uniform risk assessment template with limited national discretion to avoid fragmented procurement requirements. To provide cloud computing service providers swiftly with legal clarity, the European Commission should publish templates within three months after the ratification of the Cloud and AI Development Act. Moreover, Member States should also not be allowed to depart from the implementing acts referred to in paragraph three – otherwise, CADA is likely to jeopardise the European Commission's simplification agenda.

German industry further notes that the maximum transition period of twelve months foreseen where a risk assessment requires migration to another cloud service or assurance level does not reflect the technical reality of migrating complex services, in particular Software-as-a-Service. The maximum 12-month period in Article 29(6) should be extended to at least 24 months, with longer periods where technical complexity, continuity of essential services or contractual dependencies require it. Existing contracts should be allowed to run to expiry where risks can be mitigated, unless an urgent and substantiated public-order risk requires earlier migration. A risk-based transition period reflecting technical feasibility, service continuity and data portability would be more appropriate than a single fixed deadline.

The development of sufficient European cloud computing capacity must be regarded as a long-term objective. At the same time, fundamental changes to existing supply chains should be implemented in a gradual and pragmatic manner. Therefore, Article 29(6) should extend the maximum transition period to at least 24 months or explicitly allow the competent authority to grant extensions where the operator can demonstrate that migration within 12 months would create unacceptable operational risk for essential services.

In light of the above stated recommendations, German industry would welcome the implementation of the following amendment to the current draft law:

3. The Commission shall, by means of implementing acts in accordance with Article 46(2), *[by three months after the ratification of the legislative act]* specify the methodology to be applied,

the templates to be used and the elements to be taken into account by the Member States and Union entities for the purpose of carrying out the risk assessments referred to in paragraph 1. The methodology shall specify how Member States use the highest level of assurance for the most critical public sectors activities including, but not limited to, defence.

4. Within three months of carrying out the risk assessments referred to in paragraph 1, Member States shall provide the Commission with the results of those risk assessments, ~~indicating where they depart from the implementing acts referred to in paragraph 3.~~

Article 30 – Public procurement

Public procurement should support European resilience and innovation, while remaining competitive, technology-neutral and compatible with international trade obligations. By accounting for 14% of the EU's Gross Domestic Product (GDP), public procurement remains Europe's most powerful yet underused innovation policy tool. According to the European Commission, improving public procurement can yield big savings: even a one per cent efficiency gain could save €20 billion per year.¹ In addition, the public sector can use procurement to boost jobs, growth and investment, and to back innovative solutions developed by European businesses. The public sector must give European providers the scale required to invest, innovate and offer credible alternatives. German industry strongly supports the European Commission's intention to utilise public procurement of cloud computing services as an anchor market to increase Europe's digital sovereignty.

Article 31 – Impact assessments

German industry strongly opposes the proposal to grant the European Commission the power to impose binding requirements regarding cloud usage on individual companies of the private sector through Article 31(3). This provision should be deleted. The proposal's public-order justification is specifically linked to public procurement: Recital 64 relies on the necessary and proportionate public-order exception in Article III:2(a) of the WTO Agreement on Government Procurement. This exceptional logic cannot simply be transferred to private procurement decisions. Private-sector entities should remain free to use the framework and the Commission's guidance under Article 31(1)-(2), but the Commission should not be empowered to impose mandatory assessments and mitigation measures by delegated act. Entities referred to in Annex I of Directive (EU) 2022/2555 should be allowed to select the cloud computing service that best matches their business needs based on technical criteria and an internal evaluation of cloud computing offerings available on the market. In addition, the European Commission's proposal directly contradicts its simplification agenda as it introduces new, non-proportionate requirements onto companies.

Article 31 currently allows for extending sovereignty-related assessment obligations to private entities, including NIS2-regulated companies, through delegated acts. This option should be deleted. Such an extension is redundant, as regulated industries already conduct comparable risk assessments and implement mitigation measures under existing frameworks such as NIS2 and DORA and would therefore create duplicative compliance burden. These frameworks already address ICT third-party dependencies and therefore achieve many of the objectives that Article 31 seeks to address. Instead, the co-legislators should rely on public-sector signalling: Recital 66 already recognises that public procurement requirements influence regulated industries and generate market spillovers. Private companies have diverse risk profiles and are already subject to sectoral risk-management frameworks. It would

¹ European Commission. 2026. Public Procurement. https://single-market-economy.ec.europa.eu/single-market/public-procurement_en

also undermine commercial choice and risk encouraging third countries to introduce similar requirements, disadvantaging companies operating global networks.

German industry recommends the deletion of Article 31 (3):

~~3. Where, because of specific circumstances, and where duly justified and in consultation with the Member States, the Commission concludes that entities who are not public sector bodies operating in sectors of high criticality require an impact assessment, the Commission may adopt delegated acts to supplement this Regulation in accordance with Article 45 specifying the need for such impact assessment and the risk mitigation measures that those entities who are not public sector bodies shall take.~~

Article 32 – Union added value

German industry in general welcomes that public procurement procedures for innovative cloud computing services and AI systems shall contribute to the development of a European cloud and AI ecosystem and the uptake of respective solutions. To this end, non-price award criteria referred to in Article 32 paragraph 1 can be a suitable measure.

In applying such non-price award criteria, German industry recommends that EU value added be understood as “Made with Europe” rather than “Made in Europe”. The criteria should reward genuine European value added such as strong data protection and GDPR compliance, robust cybersecurity assurance backed by EU-based operations and threat monitoring, EU data-residency options, transparent and auditable supply chains, and sustained investment in European research, infrastructure and skills, applied transparently and on an evidence basis, without operating as “Buy European” or nationality-based preferences and without excluding providers that demonstrably meet the requirements.

Article 33 – Monitoring of procurement of innovation in cloud and AI

While German industry in general supports measures that augment the utilisation of innovative solutions developed by SMEs, a quota of at least 25% of procurement for cloud computing services and AI systems to be awarded to innovative SMEs as excessive, especially since most cloud computing services are offered by large companies.

In light of the above stated recommendations, German industry would welcome the implementation of the following amendment to the current draft law:

4. Member States shall pursue ~~the as~~-objective ~~to increase the percentage that at least 25%~~ of their procurement for cloud computing services and AI systems ~~that is be~~ awarded to innovative SMEs. Member States shall include, in their national strategies referred to in Article 7, plans on how they intend to achieve this objective.

Chapter III – European public sector cloud federation

Article 36 – Fees for the administration of the EuroCloud Federation

The voluntary public-sector cloud federation should be designed as a complementary instrument that does not distort competition with private offerings. The EuroCloud Federation under Articles 34-36 should be an interoperability and capacity-sharing layer for public bodies, not a parallel public cloud market that crowds out private European providers. It should complement competitive procurement from recognised providers and apply strict transparency and cost-accounting rules. Cost-based fees, clear participation criteria, and a focus on security and resilience are appropriate.

Chapter IV – Procurement of data centre services, cloud computing services, software and AI systems by the Commission

Article 37 – Procurement activities of the Commission

Public procurement can strengthen the European ecosystem and a resilient provider landscape, and should remain open, competitive and innovation-friendly, offering opportunities for providers of all sizes, including SMEs. The public sector should utilise its market power to function as an anchor customer for European offerings.

Chapter V – Open Source

Article 41 – Promoting open source solutions and open source first

BDI recommends replacing any mandatory 'open-source by default' requirements under Articles 41 and 42 with an enabling language that 'encourages and promotes' open source alongside proprietary commercial options, ensuring public sector buyers retain the flexibility to select the best-performing, most secure, and economically viable solutions.

Title V Final Provisions

Article 47 – Review

German industry welcomes the European Commission's aim to frequently evaluate the Regulation. However, in light of constant technological changes and geopolitical developments, we urge the co-legislators to critically evaluate whether the foreseen evaluation frequency is too long. We would recommend shortening the evaluation cycle to three years.

In light of the above stated recommendations, German industry would welcome the implementation of the following amendment to the current draft law:

1. By [date of entry into force plus 3 4 years], and every 3 5 years thereafter, the Commission shall evaluate this Regulation, and report to the European Parliament, the Council and the European Economic and Social Committee.

Annex II Criteria for Union Assurance Levels

German industry welcomes the differentiation between four Union Assurance Levels (UAL) in general as they comply with the necessary risk-based approach. The UAL should map to the sensitivity of the relevant use case. The architecture is balanced: levels 1 and 2 remain accessible to providers under third-country control where safeguards are met; level 3 is primarily reserved for EU-controlled services, with only a tightly circumscribed associated-third-country pathway under Article 18; and level 4 requires EU control. The higher assurance levels (UAL3 and UAL4) must not be diluted, as their purpose is to avoid – not merely manage – dependencies for the most sensitive use cases. Public authorities handling the least sensitive public sector data should not be subject to mandatory sovereignty requirements. Existing EU frameworks, such as NIS and GDPR, already set a high baseline for the security, resilience and availability of digital services. For many local public sector organisations and municipal service providers, this baseline is sufficient; additional requirements should only be imposed where they deliver a demonstrable security or sovereignty benefit. Local public sector organisations and municipal service providers should be provided with support to implement existing requirements to ensure that their systems are sufficiently secure and resilient.

To support digital service providers and public sector organisations, the Commission should publish practical guidance on how to carry out sovereignty risk assessments as early as possible. Such guidance should clarify which types of public sector workloads correspond to which assurance levels and should be developed with structured input from digital service providers, including SMEs. This is also necessary to prevent Member States from applying different thresholds when assessing which public sector activities require which assurance levels.

The highest assurance levels, UAL3 and UAL4, should be reserved for a clearly limited number of the most critical and sensitive public sector workloads. Although the Commission has indicated that UAL3 and UAL4 should apply only to the most sensitive share of public sector workloads, there remains uncertainty as to which public sector activities will require which assurance levels. Under CADA, the obligation to use higher-tier services is tied to activities that contribute to the preservation of public order, a notion that is left undefined and has no settled EU-law meaning; left open, it is liable to be interpreted expansively and to pull a wide range of ordinary government functions into the higher tiers. German industry therefore recommends a defined, exhaustive list of The Commission should provide guidance clarifying which types of public sector activities workloads may typically correspond to which assurance levels. BDI supports high threshold, strictly limited to the most critical use cases such as defence, law enforcement and border management, and consistent with the EU's WTO Government Procurement Agreement (GPA) commitments.

Despite the need to increase Europe's digital sovereignty, global cooperation should be encouraged. Therefore, international maintenance, remote services, technical escalation and 24/7 support must remain possible under clear safeguards, such as encryption, access control, logging and data minimisation.

German industry further notes that several criteria under Annex II warrant clarification to avoid unintended exclusions. In particular, the requirement, applicable already at the lowest assurance level to providers subject to the control of a third country, that they guarantee the absence of any third-country obligation to report software vulnerabilities to that country's authorities before exploitation, should be clarified so as not to disqualify providers subject to legitimate coordinated-disclosure or good-faith government reporting regimes in like-minded jurisdictions. Similarly, the personnel's citizenship and residency at the higher assurance levels, and the restriction on the use of service-derived data, should be applied in a manner that reflects the realities of globally operated services and does not undermine their security and resilience.

Furthermore, the term "subcontractor" in CADA's Annex II creates legal ambiguity. As currently drafted, sovereignty criteria apply uniformly to all entities involved in the provision of the audited service without differentiation based on role, data access, or actual impact on service security and continuity. This creates disproportionate compliance burdens and audit requirements that are neither proportionate to the risks involved nor matched by meaningful gains in security assurance. German industry recommends co-legislators to adopt a clear, narrow definition of "subcontractor" limited to entities that have access to, or could affect the confidentiality or integrity of, customer data or classified information processed under the audited service – directly reflecting CADA's sovereignty rationale and ensuring that localisation and audit obligations fall where the actual risk lies, rather than across the broader technology supply chain on which any modern cloud service necessarily depends.

German industry stresses that the framework should recognise the fundamental differences between the various cloud service models, in particular Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service. Requirements modelled on the Infrastructure-as-a-Service business case are frequently unworkable for Software-as-a-Service, whose reliance on cross-border data flows is often inherent to and inseparable from the service. Imposing identical requirements on structurally different

service models would disproportionately burden providers and reduce the choice available to public administrations.

Furthermore, the framework should establish a coherent and precise taxonomy of data categories, clearly distinguishing customer data from telemetry and metadata. Telemetry and metadata are frequently anonymised datasets used to maintain, operate and improve a service, and are tied to the provision of the service as a whole rather than to an individual customer. They should therefore not be subject to the same data-residency requirements as customer data, in particular not at the lowest assurance level, where such requirements would be disproportionate.

The framework should also clarify that technical and operational support, including engineering escalation (tier-3 and tier-4 support) from outside the EU, remains permissible where customer data is redacted or anonymised, so that the information shared relates solely to the technical issue and not to the customer. This would ensure that the European public sector can continue to access the best available technical support without compromising sovereignty requirements.

With regard to the highest assurance level, German industry notes that the definition of “software component”, if taken from the Cyber Resilience Act, would extend the framework's requirements to all hardware and to the software embedded within it, such as firmware and operating systems. This would de facto require an entirely EU-based hardware supply chain, which is currently not feasible, would weaken the resilience of services, and would discourage cloud adoption for more sensitive public-sector uses. The framework should clarify that its requirements do not apply to hardware or to software embedded in hardware, and the supply-chain requirements at the highest level should be aligned with those of the preceding level, which already provide strong and precise controls.

Imprint

Bundesverband der Deutschen Industrie e.V. (BDI) / Federation of German Industries
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

EU Transparency Register: 1771817758-48

German Lobbyregister: R000534

Editor

Steven Heckler
Senior Expert Cybersecurity and eGovernment
Innovation, Security and Technology
T: +49 30 2028-1523
s.heckler@bdi.eu

Lukas Kahler
Intern
Innovation, Security and Technology
T: +49 30 2028-1461
l.kahler@bdi.eu

Philipp Schweikle
Expert Digital Infrastructure and International Digital Policy
Innovation, Security and Technology
T: + 49 30 2028-1632
p.schweikle@bdi.eu

Dr Michael Dose
Senior Expert Data Policy and Data Protection
Innovation, Security and Technology
T: +49 30 2028-1560
m.dose@bdi.eu

Document number: D 2342