Brussels, November 2026

BSP Position Paper: Cloud and AI Development Act (CADA) – feedback

Business & Science Poland

This position paper is submitted on behalf of Business & Science Poland (BSP) as feedback on the European Commission's published legislative proposal for the Cloud and AI Development Act (CADA). It provides an industry perspective on the proposed provisions, highlighting key concerns and recommendations based on practical business experience. The following paper incorporates insights from the "EU Tech Sovereignty Package in Focus" roundtable held on 24 June 2026, which brought together representatives of the European Commission, the European Parliament, Polish and Czech administrations, industry associations, technology companies from Central and Eastern Europe, and institutions supporting innovation.

Background

The proposed Cloud and AI Development Act (CADA) gives the European Union the chance to go further than regulating technology and create the conditions in which European businesses can develop, acquire and deploy that technology at scale. Business & Science Poland (BSP) shares the European Commission's aim of expanding the Union's computing capacity, strengthening its cloud and AI ecosystem and reducing critical technological dependencies. Technological sovereignty should mean that European public institutions and businesses are able to maintain essential services, control material risks, select appropriate technology suppliers and avoid dependencies they cannot manage. The June 2026 BSP roundtable conveyed a consistent practical message: investment, faster deployment, access to electricity and connectivity, demand for competitive solutions and better access to finance will determine whether Europe's technological ambitions succeed. Achieving this requires a level playing field in which European customers retain access to the most secure and innovative services available, on competitive terms, while measures to reduce dependencies should open up real opportunities for European providers without unduly limiting choice or lowering the quality of services open to European businesses and innovators. BSP therefore supports CADA's objectives on capacity-building and innovation and asks that its provisions on sovereignty and procurement be applied in a way that is proportionate, operationally workable and encourages investment. These points carry weight for entities in the sectors of high criticality listed in Annex I to the NIS2 Directive and for industrial users of cloud and AI services.

Rue Belliard 40, 1000 Brussels
e-mail: info@zpbsp.com
EU Transparency Register Number: 548212735276-89

Key BSP recommendations

- Ensure that national cloud and AI strategies are operational and supported by implementation plans
- Base the designation of acceleration zones on consistent criteria that include demand
- Ensure a justified and proportionate allocation of Union assurance levels (UALs)
- Prevent new supplier dependencies and preserve operational continuity
- Maintain a voluntary risk-assessment framework for private-sector operators to limit uncertainty for critical private-sector operators
- Maintain Member States' responsibility for determining Union Assurance Levels
- Ensure transparent, safeguards-based decisions on third-country eligibility for UAL 3
- Prevent cumulative regulatory obligations and fragmentation of the Single Market

Detailed recommendations

Technological sovereignty should mean the EU's ability to develop and maintain critical digital infrastructure, keep essential services running and reduce its strategic dependence on external technology providers. BSP sees the following as the main ways to achieve this:

(1) **Ensure that national cloud and AI strategies are operational and supported by implementation plans [Article 7].** Article 7 requires each Member State to adopt a national cloud and AI strategy within one year of the Regulation's entry into force. Each strategy must set out objectives and priorities for cloud and AI adoption, together with a governance and monitoring framework. It must also include measures in areas such as cloud and AI adoption by public sector bodies, SMEs and small mid-caps, data centre capacity, investment in high-intensity computing infrastructure and the deployment of AI in industry. Yet greater transparency regarding available financing and infrastructure would help companies plan investments and facilitate the industrial deployment of AI, particularly among SMEs. National strategies should therefore identify, for each measure, the available financing instruments, the responsible authority and an indicative implementation timeline and should be made publicly available. This should also apply where a Member State relies on an existing strategy instead of adopting a new one.

(2) **Base the designation of acceleration zones on consistent criteria that include demand [Articles 10-13].** For CADA to attract investment in data centres in Europe, the rules on acceleration zones, permitting and strategic projects must tackle the main barriers to deployment: slow administrative procedures, limited access to energy and network infrastructure, and investment uncertainty. The measure of success should be how quickly new computing capacity comes into operation. The Central and Eastern European (CEE) region has a strong technology sector, built on the expertise of local companies and projects that could support the industrial-scale deployment of AI. Realising this potential will, however, require better access to financing and a stable, predictable regulatory framework. In this context, we particularly welcome the Commission's ambition to triple data centre capacity in the EU within five to seven years, as well as the proposed acceleration zones with simplified permitting procedures, a 12-month deadline for granting permits, an aggregated baseline permit mechanism, single information points and forward-looking grid planning that takes future energy demand into account. Nevertheless, we see several challenges in implementing these measures. When designating acceleration zones under Article 10, Member States should consider demand-side indicators, particularly actual demand for computing capacity, alongside supply-side factors such as grid capacity and on-site clean energy generation. Designating zones without assessing demand risks directing investment towards economically suboptimal locations. The Commission should also provide guidance to Member States on the designation criteria set out in Article 10 to prevent fragmentation, whereby comparable sites could qualify in one Member State but not in another. Furthermore, the sustainability requirements under Article 11 should also be aligned with the performance classes of the EU data centre rating scheme for power usage effectiveness (PUE) and water usage effectiveness (WUE), and take account of the renewable energy factor (REF). Finally, acceleration zones should accelerate rather than hinder development. Treating them as isolated, self-contained areas could discourage investment outside designated zones, lead to speculative increases in land prices within them and concentrate the development of computing capacity in a limited number of locations, rather than generating a more balanced expansion of computing capacity and broader spillover effects.

(3) **Ensure a justified and proportionate allocation of Union assurance levels (UALs) [Article 29(1)–(3)]**. Article 29 requires Member States to conduct risk assessments and determine the appropriate UAL for relevant public-sector activities. Risk assessments should therefore provide a reasoned justification for assigning UAL 3 or 4 to given categories of public-sector activities. The common methodology under Article 29(3) should establish clear criteria for determining when higher assurance

levels are necessary, considering data sensitivity and protection, technical and operational controls, operational criticality, risks of unauthorised third-country access or interference, service continuity and existing safeguards. The assessment should demonstrate why a lower assurance level would not adequately address the identified risks. Article 29 of the proposal does not explicitly require Member States to explain why UAL 2 would be insufficient before assigning UAL 3 or 4. More clearly defined criteria would improve consistency across Member States, reduce uncertainty and ensure that higher assurance levels are applied where necessary to address identified risks. This would preserve strong protection for critical public-sector activities without imposing disproportionate requirements on less sensitive applications.

(4) **Prevent new supplier dependencies and preserve operational continuity [Articles 29(6); 29(9)].** Enable effective multi-cloud options, exit planning and migration arrangements proportionate to technical reality. Require public-sector risk assessments to consider supplier concentration, interoperability and the availability of suitable alternative services, alongside the operational implications of switching providers. Where appropriate, multi-vendor and multi-cloud arrangements should be used to reduce dependency risks, supported by workable exit strategies and technically feasible migration arrangements. Article 29(9) already requires risk assessments to consider whether a multi-vendor or multi-cloud strategy is appropriate, and Article 29(6) requires any necessary migration to be completed within a transition period of no more than 12 months, taking into account technical feasibility, continuity of service and data portability. However, Article 29 does not require risk assessments to consider supplier concentration or the availability of suitable alternative services. Reducing reliance on third-country providers should not result in new forms of market concentration or operational vulnerability. Assessing supplier availability, interoperability and migration feasibility would help public authorities manage technological dependencies while supporting the development of competitive alternatives.

(5) **Maintain a voluntary risk-assessment framework and limit uncertainty for critical private-sector operators [Article 31(1)–(3)].** Article 31 must not become an open-ended route for extending public-sector sovereignty requirements to entities covered by Annex I to the NIS2 Directive without sector-specific justification, consultation with affected businesses and an assessment of cost and continuity implications. Article 31(1) allows private-sector entities covered by Annex I to the NIS2 Directive to conduct voluntary cloud-sovereignty risk assessments. However, Article 31(3) would empower the Commission, where it considers this duly justified

and after consulting Member States, to require mandatory assessments and risk-mitigation measures for private entities in sectors of high criticality through delegated acts. This creates significant legal uncertainty. We recommend deleting Article 31(3) in its current form. Private operators in critical sectors are already subject to cybersecurity and operational resilience obligations under NIS2, DORA where applicable, and sector-specific legislation. Additional mandatory assessments and mitigation measures could duplicate existing obligations, increase compliance costs and create uncertainty for long-term technology investments. Any future extension of mandatory cloud-sovereignty requirements to private-sector operators should be subject to the ordinary legislative procedure, following a sector-specific impact assessment and consultation with affected businesses. Extending these obligations could prompt costly reassessment, contract renegotiation, system redesign and rushed migrations that themselves create security and operational risk, duplicating obligations these sectors already meet under NIS2, DORA and sector-specific law.

(6) **Maintain Member States' responsibility for determining Union assurance levels [Article 29(5); Article 4(2) TEU].** Article 29(5) would allow the Commission, by means of implementing acts, to impose a different UAL from the one a Member State has determined in its risk assessment, where the Commission concludes that the national level is not appropriate or does not adequately address public order concerns**.** The risk assessments cover activities in areas such as national security, defence and law enforcement, and under Article 4(2) TEU national security remains the sole responsibility of each Member State. We therefore recommend removing this power. Alternatively, it should be strictly limited to clearly defined circumstances and made subject to a reasoned justification and appropriate procedural safeguards.

(7) **Ensure transparent, safeguards-based decisions on third-country eligibility for UAL 3 [Article 18; Annex II, point 3.1(g)].** Providers controlled by a third country or a legal entity established in a third country are generally excluded from UAL 3 unless the Commission has recognised the relevant third country under Article 18. Such recognition only allows providers to be audited against the UAL 3 criteria and it does not automatically grant that assurance level. Article 18(3) only requires the Commission to publish a list of the third countries that meet the criteria and of those that no longer do. It would be recommended to require the Commission to publish a reasoned assessment against each criterion under Article 18(1). Article 18(2) requires the Commission to repeal, amend or suspend a recognition decision where the relevant conditions are no longer met. The Regulation should specify the

consequences for services already recognised at UAL 3 and provide proportionate transition arrangements.

(8) **Prevent cumulative regulatory obligations and fragmentation of the Single Market [Articles 16, 17, 20, 21, 25 and 29; Annexes II and III].** CADA's assurance framework, audits, cloud procurement rules and risk assessments should be aligned with NIS2, the Cybersecurity Act framework and the Data Act, with a clear division of responsibilities and no unnecessary duplicate evidence requests. CADA would add a further layer of requirements to an already complex body of EU regulation, including a new cloud sovereignty framework with four assurance levels, audits and recognition procedures for cloud providers, risk assessments, public procurement criteria and reporting obligations, as well as new tasks for national competent authorities. Although CADA provides for a common EU risk-assessment methodology, differences in its application across Member States could lead to divergent sovereignty requirements. If the 27 Member States carry out their risk assessments differently, the result could be 27 different national approaches to sovereignty. This would undermine the economies of scale needed to attract around EUR 200 billion in mostly private investment, create uncertainty for long-term investment and run counter to the Draghi Report's recommendations on reducing regulatory burdens.

(9) **Clarify the legal and operational requirements under the Union assurance levels [Article 16; Annexes II and III].** The UAL framework also raises concerns about the legal concepts it uses. In particular, the notion of 'resilience to non-EU jurisdiction' lacks legal precision, given that global cloud providers operate under multiple jurisdictions, including within the EU. Furthermore, Annex II requires customer data, including metadata and telemetry data, to remain exclusively within the EU unless the public sector body explicitly requires otherwise. However, the proposal describes 'customer data' only in indicative terms, and that description extends to data under the provider's control that results from the customer's use of the service. The scope of customer data therefore remains unclear, particularly where it may include operational data that providers generate for cybersecurity purposes. Data localisation alone does not guarantee security or resilience. Ukraine's experience shows the importance of geographically distributed cloud infrastructure for maintaining service continuity during physical disruptions.

Conclusion

BSP supports an ambitious CADA that aims to turn Europe's technological sovereignty agenda into more computing capacity and more resilient cloud and AI services. The final shape of the Regulation should allow Member States and businesses to manage real dependencies without putting operational continuity at risk or slowing down the adoption of new technologies. The overall priority should be a workable framework that speeds up projects and widens choice, not one that mainly adds new risk assessments. If the EU wants to make a real change in how it builds sovereign technology, it will need to go well beyond simplifying rules and adjusting compliance requirements. It needs instruments that build industrial capability, strengthen demand for European solutions and help businesses take up new technology faster.

About BSP

Business & Science Poland (BSP) combines the experience of leading Polish enterprises with the EU agenda. We represent the knowledge and interests of Polish companies employing over 280,000 people in Poland, the EU, and globally. Our goal is to support the EU Single Market in line with the need for its responsible and effective transformation. This opinion presents the position of BSP members representing the digital, financial, air transport, fertiliser, chemical, mining, refining, fuel and energy sectors.

Rue Belliard 40, 1000 Brussels
e-mail: info@zpbsp.com
EU Transparency Register Number: 548212735276-89