

Building Europe's cloud and AI capacity:
how insurers can support investment and resilience

Insurance Europe welcomes the strategic objectives of the Cloud and AI Development Act (CADA) to strengthen Europe's cloud and AI ecosystem by increasing computational capacity, boosting innovation, accelerating AI adoption and building cloud and data infrastructure.

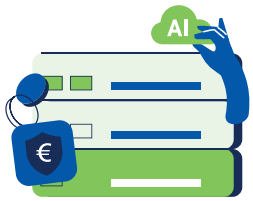
CADA can help to create the right conditions for the EU to incentivise large investments and increase the EU's current cloud and data centre capacity to meet the needs of businesses and public administrations across the entire EU. The insurance industry supports such a focus.

Enhancing Europe's digital and technological prowess requires a regulatory framework that fosters investment, innovation and competitiveness. The long-term objective should be to ensure that European solutions and alternatives are globally competitive, enabling them to broaden the range of available market offerings in a sustainable and effective manner.

The role of insurers

Insurers can support Europe's cloud and AI goals in two significant ways

Infrastructure investment: financing long-term growth



€9.5 trillion
assets under management

- Long-term institutional investors
- Financing strategic digital infrastructure
- Supporting Europe's digital transitions

Insurability of data centres



Insurance + risk expertise

- Coverage for data-centre projects
- Early risk identification and mitigation
- Supporting resilient design and long-term insurability

The insurance sector can make an important contribution to the goals of CADA in two significant ways: as a long-term institutional investor in digital infrastructure and as a provider of insurance coverage and risk management expertise for data-centre projects.

Infrastructure investment: financing long-term growth



Insurance companies are among Europe's largest long-term institutional investors. With approximately EUR 9.5 trillion in assets under management, the insurance sector is uniquely positioned to contribute to Europe's digital transition by providing long-term financing to strategic infrastructure projects across the EU.

Digital infrastructure, such as data centres, is increasingly becoming as strategic to Europe's competitiveness and sovereignty as traditional energy and transport infrastructure. The challenge, however, does not lie in a lack of available capital, but rather in the availability and predictability of sufficiently large, investment-ready projects that enable institutional investors to deploy capital efficiently and at scale.

The insurance industry welcomes the approach under CADA to designate data centre acceleration zones and to streamline administrative and permit-granting processes for the deployment of data centre projects. Accelerating permitting and project approval procedures across Member States is crucial, as lengthy and complex permitting procedures remain a major obstacle to project delivery in many Member States. Improving coordination between public authorities and reducing administrative bottlenecks can shorten development timelines, improve project visibility and accelerate the deployment of private capital, particularly in strategic sectors such as digital infrastructure.

To unlock insurers' full potential as long-term infrastructure investors, Europe must focus on creating a predictable and scalable pipeline of investment-ready projects. In addition to faster and more efficient permitting procedures for the building of data centres, a comprehensive European public–private partnership policy framework should be developed with the support of the European Investment Bank and other public institutions, to facilitate risk sharing, improve project delivery and crowd in private capital rather than crowding it out. In this regard, we recommend implementing the proposal from the Letta Report for a European Framework for Public Private Partnerships (page 31), which would help ensure a balance between affordability for taxpayers and profitability for investors, and overcome a certain bias against PPPs from a fiscal perspective.

Insurability of data centres



The insurance industry supports CADA's objective to at least triple the EU's data centre capacity within the next 5 to 7 years. Under certain conditions, data centres are insurable by the private market, and insurance can support Europe's build-out across various projects.

At the same time, the scale, speed and increasing complexity of the planned build-out are changing the risk profile of data centre projects. Early engagement with insurers can help identify and address potential risks as projects are designed and developed, supporting resilient construction and long-term insurability.

Insurability also depends on the resilience of the infrastructure and supply chains on which data centres rely. This includes electricity grids, water consumption and cooling systems, telecom and cloud infrastructure, and specialised equipment such as semiconductors and transformers. Fire risks, including those associated with battery energy storage systems, as well as environmental considerations, including water availability and natural-catastrophe exposure, can further affect the resilience and risk profile of individual sites. Geographic concentration and shared infrastructure dependencies can create additional risks, making resilient design and appropriate site selection important. Operational resilience also depends on access to critical software, including updates, licenses and technical support, which could be disrupted by geopolitical or regulatory developments.

CADA should therefore support resilient design and infrastructure, technically precise risk information and efficient data sharing, as well as sufficient flexibility for insurers and clients to structure appropriate coverage solutions. Together, these conditions will help support insurability and enable private insurance capacity to support the European data-centre build-out.

European digital sovereignty



It is essential that businesses can continue to make use of the services that deliver the greatest value, rather than being forced to disconnect from them. Digital sovereignty is not about isolating Europe but should be achieved through effective oversight and clear rules for providers, while preserving access to global technologies that are essential for European competitiveness, resilience and innovation.

The focus of enhancing Europe's technological sovereignty should be on investment in R&D, infrastructure and cloud and AI capabilities, as suggested in the Commission's approach. European sovereignty can only be successfully achieved through capacity-building and creating the right foundations for European businesses to thrive.

While there may be merit in further exploring the possibility of enhancing Europe's digital sovereignty, this should be a longer-term policy discussion at EU level with an appropriate focus on increasing investment and building capacity and infrastructure, rather than an approach that seeks to place restrictions on the private sector in its choice of providers. The European cloud market is not sufficiently mature, and it will take time for European providers to reach the level of technical capability of the US hyperscalers. Proposing to attain European sovereignty without the necessary capacity and infrastructure in place will not achieve the desired outcome.

The insurance industry encourages policymakers to ensure that the following elements are a clear focus of CADA:

- continued access to best-in-class technology to ensure European businesses remain globally competitive;
- a clear, risk-based definition of "sovereign cloud" that allows for compliance through contractual, operational, and technical safeguards rather than jurisdictional exclusion;
- flexibility for hybrid and multi-cloud strategies, to enable user choice and prevent market lock-in;
- creating incentives for the voluntary use of sovereign solutions, while allowing European insurers to retain their freedom of choice regarding cloud and AI providers, exercised through their own governance and a risk-based approach, within an already robust sectoral regulatory framework;
- a focus on interoperability and innovation, to preserve Europe's competitiveness and prevent market fragmentation; and
- direct obligations for providers rather than indirect obligations imposed on insurance undertakings.

It is crucial that support for developing cloud and AI in Europe does not translate into an obligation on the private sector to use European or "sovereign" providers. Any such obligation would entail additional costs, would reduce full access to the most cutting-edge technologies and could ultimately lead to a step backwards for EU businesses in terms of competitiveness, digital innovation and security. This would be particularly detrimental to European businesses, including insurers, with significant operations outside the EU, which need continued access to global cloud services irrespective of improvements in EU cloud capacity.

Such an obligation should also be avoided where insurers provide insurance services to public entities or their personnel and may process public-sector data as part of an insurance contract. Article 32 requires contracting authorities procuring innovative cloud computing services and AI systems to assess contributions to the European cloud and AI ecosystem, including the use of EU-developed technologies and EU-designed or manufactured hardware and software; while these criteria should remain ancillary, their application could create de facto European-origin requirements and restrict insurers' access to best-in-class technologies for cyber security, fraud prevention, claims handling, automation and risk modelling. Article 32 should therefore be applied proportionately, taking account of market availability and technical requirements, and should not impose additional sovereignty requirements on insurers through procurement procedures or contractual conditions.

In some Member States, insurance companies may perform limited public-sector functions when providing mandatory insurance, such as motor third-party liability and workers' compensation insurance. This ancillary role should not bring a private-sector entity within the scope of obligations intended for public-sector bodies, as this could create local fragmentation, unintended consequences for the private sector and barriers for insurance companies offering certain insurance products.

To preserve CADA's intended function as a coherent single market instrument, its scope and other key provisions should be fully harmonised across the EU, with national discretion limited to what is strictly necessary. A uniform framework would prevent divergent national regimes and unnecessary burdens for organisations operating in several Member States.

Consistency with the Digital Operational Resilience Act (DORA)

At the same time, CADA must be implemented in a way that is fully consistent with the existing sectoral framework for financial entities. EU financial services legislation already imposes comprehensive requirements on financial entities regarding the management of risk, including operational risk. For insurers, the Digital Operational Resilience Act (DORA) is the governing framework for ICT risk management, ICT third-party risk, cloud outsourcing, contractual safeguards, concentration risk, exit strategies, testing and supervisory oversight. The CADA proposal itself recognises that DORA has a sectoral scope specific to the financial sector.



To ensure legal certainty and avoid unnecessary burden, the legislative proposal should clarify the following:

- CADA is without prejudice to DORA and does not create additional ICT risk management, outsourcing, contractual, reporting, testing or supervisory obligations for insurance and reinsurance undertakings. There is a risk that an expanded scope of CADA, cf. art. 31 (3), could result in overlapping requirements and a further fragmented regulatory landscape. Duplication in obligations across regulation or overlapping requirements will increase administrative burdens, including increased costs related to documentation, contract management, vendor management, audits, and any migration or adaptation processes, and would run counter to ongoing legislative efforts, such as the Digital Omnibus and the Digital Fitness Check, which are specifically aimed at simplifying and streamlining the EU regulatory landscape.
- CADA, and Article 31 in particular, should remain voluntary for all private entities and should not apply to financial entities subject to DORA. This would ensure consistent treatment of DORA-regulated financial entities and avoid divergent requirements within the same sector depending on whether an entity falls within the scope of NIS2. Sovereignty requirements under CADA should not restrict insurers' choice of cloud service providers where this could undermine DORA compliance, operational resilience or customer data security, nor result in forced migration to European providers. However, DORA-regulated entities may choose to incorporate elements from CADA into their internal risk management processes as supplementary measures. Any such use should complement existing requirements and preserve the risk-based approach and principle of proportionality embedded in DORA and other relevant legislation, such as the GDPR. Any Commission guidance or delegated acts on private-sector impact assessments should avoid duplicating DORA requirements and be developed in consultation with the ESAs and relevant industry stakeholders. Similarly, CADA-recognised assurance levels should remain optional evidence that may support DORA due diligence, contract management and exit planning, rather than becoming mandatory conditions for insurers' use of cloud services.

- In some Member States, insurers may provide, organise or coordinate certain healthcare services for claimants as part of the claims handling process, including rehabilitation and care planning, and may consequently be required to register as healthcare providers under national law. These limited activities should not affect their status as financial entities whose ICT and cloud arrangements are already comprehensively regulated under DORA. CADA should therefore clarify that performing such healthcare-related activities, or holding the corresponding national registration, does not in itself bring insurers within its healthcare-related scope or create additional requirements.
- Consideration should also be given to whether recognised providers could, on request, share summarised audit evidence with public and private users needing more than an audit conclusion for due diligence under DORA or other Union law. This could cover infrastructure, asset and personnel locations, evidence of Union-only customer data storage and processing, including third-party safeguards, and a summary of the software bill of materials, including open-source components, subject to the confidentiality safeguards in Article 20(3). Alternatively, CADA should clarify that positive audit opinions at Union assurance levels 2, 3 or 4 may serve as evidence in, or partial fulfilment of, that due diligence, without prejudice to users' own responsibilities.

A clear lex specialis safeguard for DORA is essential to ensure that CADA supports innovation and resilience without increasing regulatory fragmentation or compliance burden for insurance undertakings.

Insurance Europe is the European insurance and reinsurance federation. Through its 39 member bodies — the national insurance associations — it represents insurance and reinsurance undertakings active in Europe and advocates for policies and conditions that support the sector in delivering value to individuals, businesses, and the broader economy.

November 2026

insurance europe
www.insuranceeurope.eu
Insurance Europe
Rue du Champ de Mars 23
B-1050 Brussels - Belgium