Copyright©2026EuropeanDIGITALSMEAlliance

European DIGITAL SME Alliance

SEPTEMBER 2026

POSITION PAPER

# Cloud and AI Development Act

**CONTACT** P - +32 28930235 E - office@digitalsme.eu **ADDRESS** Rue Marie Thérèse 21 bte.5 1000, Brussels Belgium

# EXECUTIVE SUMMARY

In June 2026, the European Commission has published the Tech Sovereignty Package, with the Cloud and AI Development Act (CADA) as one of its key components.

The CADA is a legislative proposal representing an important step towards a more proactive European industrial strategy aimed at strengthening Europe's capabilities in cloud and artificial intelligence technologies while reducing strategic dependencies on non-European providers.

The proposal introduces a comprehensive set of measures to boost Europe's cloud and AI ecosystem. These measures encompass the establishment of the Union Cloud Sovereignty Framework, including a reopening of the European Cloud Cybersecurity Scheme (EUCS), as well as initiatives to accelerate the deployment of cloud and AI infrastructure, procurement mechanisms that reinforce European added value.

The European DIGITAL SME Alliance welcomes this direction. This position paper analyses the most critical components of the CADA proposal and sets out key recommendations to ensure that the implementation of the CADA effectively strengthens Europe's digital ecosystem and enables the broad adoption of sovereign solutions.

The legislation must ensure that sovereignty thresholds are meaningful in practice, that SMEs can access certification and procurement opportunities on proportionate terms, and that demand-side measures extend beyond public procurement to the private sector, and that Europe's fragmented provider landscape is federated into a market capable of competing at scale.

## DIGITAL SME's headline recommendations are:

- **Strengthen the Union Cloud Computing Sovereignty Framework and protect Level 3 as a genuinely European-control threshold.** Level 3 should be reserved for European-controlled providers, with stronger safeguards against structures that preserve effective third-country influence.
- **Increase SME participation in public procurement.** Raise the SME procurement target from 25% to 35%, remove the undefined qualifier "innovative", and introduce ex-ante SME Compliance Tests for tender requirements.
- **Create a measurable European preference trajectory.** Require at least 50% of public administrations' cloud services to be sourced from providers recognised at Union assurance Level 3 or above by 2030, with annual monitoring.
- **Stimulate private-sector demand.** Establish an EU-wide SME Digitalisation Voucher Scheme for sovereign solutions and use Article 31 to extend sovereignty assessments to private operators in sectors of high criticality.
- **Federate the European cloud market.** Open the EuroCloud Federation to trusted European private providers, and mandate common APIs and standards so that Europe's many providers can be consumed as a single addressable market, backed by a joint political and industrial commitment along the lines of the 1987 GSM Memorandum of Understanding.
- **Align infrastructure incentives with sovereignty objectives.** Condition acceleration-zone benefits and strategic-project designation on European control and reserve a meaningful share of capacity for SMEs.
- **Build an EU Tech Catalogue inclusive of all European-controlled solutions.** The Tech Sovereignty Catalogue could serve as a basis for developing such an inclusive framework.

# TABLE OF CONTENTS


1. Cloud computing sovereignty framework - Key provisions.....5
    a. Use of public procurement to boost sovereign cloud uptake.....6
2. Cloud computing sovereignty framework - Governance and implementation.....8
3. Demand-side measures.....10
4. Federation of the European cloud market.....11
5. Data Centre Capacities.....12
6. EuroCloud Federation.....14
7. Open Source and the EU Solutions Catalogue.....15
8. Conclusion.....16

# 1. Cloud computing sovereignty framework - Key provisions

## CADA proposal

Title IV, Chapter I, establishes a single, EU-wide cloud computing sovereignty framework, setting out four auditable levels of sovereignty in line with the requirements defined in Annex II. Under the proposal, providers shall apply to the national competent authority for certification, and non-EU providers may also participate provided they meet specific cumulative compliance requirements. Level 1 relies on standardised self-assessment, while Levels 2 to 4 require certification by accredited auditors. Member States and Union entities shall carry out risk assessments to determine the applicable level.

## DIGITAL SME assessment

DIGITAL SME welcomes the pragmatic approach adopted by the Commission on the basis of the Cloud Computing Sovereignty Framework described above. Establishing auditable levels of sovereignty, and recognising that the jurisdiction, ownership and operational control of digital infrastructure carry strategic consequences, marks a necessary departure from procurement practices built primarily around cost.

But the value of the framework rests entirely on whether the four levels differ materially in practice rather than only on paper.

Level 1 relies on self-assessment and allows public bodies to waive both infrastructure and data localisation, which places it close to current market practice.

Level 2 permits a provider subject to third-country control to qualify by documenting legal, technical and organisational separation measures, which is the architecture that large non-EU providers are already trying to build into their European offerings.

The framework's first real break with extraterritorial exposure therefore occurs at Level 3, and the integrity of the whole structure depends on how that threshold is defined and how access to it is governed.

## DIGITAL SME recommendations:

- **Reserve Level 3 for European-controlled providers.** The criteria governing the designation of associated third countries under Article 18 are insufficiently defined and adopted in agreement with the Member States, which leaves a determination of considerable strategic consequence to political discretion. In particular, Adequacy under Article 45 GDPR addresses international transfers of personal data and cannot resolve exposure to extraterritorial legislation or to divergent sanctions regimes. The co-legislators should either exclude third-country designation from Level 3 entirely, leaving Article 18 recognition to apply at Level 2, or define the criteria more clearly in the legislative text.

- **Prevent sovereignty washing.** The control tests in Annex II and Annex III should be strengthened to capture joint ventures and minority stakes that confer effective influence over strategic decisions, so that a non-EU provider cannot reach Level 3 by restructuring below the ownership threshold while retaining operational and technical control. Effective European control should be demonstrated across infrastructure, personnel, technical support, management planes, cryptographic material and continuity procedures, rather than inferred from the shareholding structure alone.

- **Preserve genuine differentiation between sovereignty levels.** Each level must correspond to a materially different degree of sovereignty guarantee, without room for interpretation, with higher levels providing real protection against extraterritorial interference.

# a. Use of public procurement to boost sovereign cloud uptake

## CADA proposal

Article 30 makes the assurance level identified through the risk assessments binding in public procurement, requiring contracting authorities whose activities do not contribute to the preservation of public order to use services recognised at Level 1, and those whose activities do to procure exclusively at Level 2, 3 or 4, subject to exemptions where no recognised service can meet the subject matter of the contract. Article 33 requires Member States to monitor and report annually on the size of participating economic operators and on trends in SME participation, sets the objective that at least 25% of cloud and AI procurement be awarded to innovative SMEs, and calls for preliminary market consultations, matchmaking between public buyers and innovative European SMEs and start-ups, and contract clauses favourable to innovative SMEs.

## DIGITAL SME assessment

The introduction of non-price criteria for cloud procurement, marks a departure from procurement models based primarily on cost considerations, recognising that the governance, jurisdiction, and control of digital infrastructure carry strategic implications for Europe's resilience.

Innovative SMEs, start-ups and scale-ups play a vital role in Europe's cloud and AI ecosystem. Public procurement can help create the conditions for their growth and expansion, while promoting competition and contributing to a more diversified and less concentrated market, even when it comes to the production of sovereign technologies.

Therefore, aiming to promote a higher participation of SMEs in public tenders and promoting strict sovereignty requirements in public tenders on digital services and products are objectives that can go hand-in-hand. At the same time, targets of this kind will only shape behaviour if achievement can be measured consistently and someone is accountable for it, and Article 33 currently provides for reporting in general terms without specifying the granularity, comparability or institutional responsibility needed to make the objective operational.

### DIGITAL SME recommendations:

- **Increase the SME participation target to 35%.** The 25% target for procurement from innovative SMEs in Article 33(4) provides a solid starting point. However, the CADA proposal should adopt a more ambitious objective by increasing the target to 35%. In addition, the qualifier "innovative" should be removed, as it narrows the target to an undefined subset of SMEs. Achieving this level will require targeted measures to enable SME participation, including dedicated support programmes with proportionate qualification and eligibility criteria tailored to the capacities of SMEs.

- **Make the target verifiable and accountable.** Each Member State should publish a standardised annual monitoring report setting out the actual share of cloud and AI public procurement awarded to SMEs, in a format comparable across the Union, since a general monitoring mechanism will not allow progress towards the target to be verified in practice. Member States should also designate a competent authority responsible at national level for implementing and monitoring the SME objective, working alongside the national SME Envoy, whose network is a valuable channel for feedback and does not carry a mandate to act where the target is not met.

- **Introduce ex-ante "SME Compliance Tests".** Procurement requirements should be assessed before to determine whether they enable effective SME participation. Results should feed into the annual monitoring mechanism under Article 33(1) to (3) and reflected in the national strategies foreseen in Article 7.

- **Set a measurable European preference target.** The same monitoring framework should carry an objective requiring that at least 50% of public administrations' cloud services are sourced from providers recognised at Union assurance level 3 or above by 2030, reported annually by Member States and planned for in their national strategies. The co-legislators should accompany this target with a clear implementation trajectory so that progress can be assessed consistently.

## 2. Cloud computing sovereignty framework - Governance and implementation

### CADA proposal

Under Title IV, Chapter I, Section 2, recognition under the Sovereignty Framework is granted by national competent authorities under Article 17, on the basis of a self-assessment at Level 1 or an independent third-party audit at Levels 2 to 4. Article 20 places the cost of that audit on the provider and sets the conditions applying to auditing organisations, requiring independence, absence of conflicts of interest, proven expertise and proven objectivity.

Annex III forms the operative basis on which auditors assess compliance with the Annex II criteria, and Article 16 empowers the Commission to amend both annexes by delegated act while requiring it to review them at least every 18 months. Recognised services are listed in a central repository maintained by the Commission, and the methodology for the underlying risk assessments is to be specified through implementing acts.

### DIGITAL SME assessment

Much of what CADA's practical effect sits below the level of the legislative text. The criteria defining each assurance level, and the evidence against which compliance is judged, are both set out in annexes that the Commission may amend by delegated act, which means the practical substance of sovereignty will be settled through delegated and implementing acts, periodic revision, and the professional judgment of auditors rather than in the trilogue on the articles themselves.

The 18-month review obligation is a welcome acknowledgement that these requirements cannot remain static, since sovereignty risks move quickly across extraterritorial legislation, management plane architectures, key management practice, AI infrastructure dependencies and portability constraints. It says nothing, however, about how that review is conducted, who contributes to it, or what triggers an amendment, and a requirement drafted in those terms can be discharged without any external input.

The audit ecosystem carries a comparable weakness. Applying the same audit procedure at the provider's own expense irrespective of size falls hardest on the smaller European companies the framework is meant to strengthen. Holding auditing organisations to qualitative conditions alone, with no accreditation, no register and no supervisory structure behind terms such as proven expertise, means the same criteria will be applied by 27 national authorities relying on auditors held to a standard the Regulation never defines. Divergence then becomes a competitive variable between Member States. Recognition at a given assurance level should mean the same thing across the Union, and it should be attainable by companies of every size.

## DIGITAL SME recommendations:

- **Introduce a proportionate pathway for SMEs.** Article 20 should differentiate audit requirements by provider size and risk profile, including simplified evidence requirements for defined service categories and support to offset audit costs for SMEs seeking recognition at Level 2 and above.
- **Ensure transparent methodologies and structured stakeholder involvement.** The 18-month review under Article 16(3) should be public and evidence-based and supported by a structured public-private expert mechanism covering interpretation issues, emerging sovereignty risks and the adequacy of audit evidence, with guaranteed representation for SMEs. A European stakeholder forum, adequately representing EU-controlled SMEs and innovators in the area of cloud, should be established to achieve this goal.
- **Harmonised interpretation across Member States**. Auditing organisations should be accredited by national accreditation bodies under Regulation (EC) No 765/2008 or an equivalent Union framework, with a public register of accredited organisations, so that recognition carries the same meaning in every Member State.

# 3. Demand-side measures

## CADA proposal

In Title IV, Chapter II, the proposal establishes demand-side measures to stimulate the adoption and deployment of cloud and AI solutions across the European economy. Under Article 29, Member States and Union entities must carry out periodic risk assess-ments identifying which public sector activities contribute to the preservation of public order, and Article 30 makes the resulting assurance level binding in procurement.

Article 31 allows private entities in NIS2 sectors to carry out equivalent assessments on a voluntary basis, and empowers the Commission to make them mandatory for sectors of high criticality by delegated act. Article 32 requires contracting authorities to apply non-price award criteria assessing a tenderer's contribution to the European cloud and AI ecosystem.

## DIGITAL SME assessment

CADA's demand-side measures are a welcome first step, recognising that stimulating demand matters as much as building supply. The chapter is nonetheless built almost entirely around public procurement. Nothing in the chapter creates an incentive, an obligation or a funding instrument capable of moving private-sector demand, which leaves the entire demand side of the proposal resting on public contracts. Public sector cloud spending accounts for a modest share of the European market, so even a fully effective procurement mandate would leave the bulk of demand untouched and would not generate the volume European providers need to reach competitive scale.

The instruments are also weaker than they first appear. The non-price award criteria under Article 32 remain ancillary and not decisive, which caps the European added value lever by design and prevents it from determining outcomes. Article 31 meanwhile contains a delegated power capable of extending sovereignty assessment to critical private-sector operators, and it is not clear whether it will be used. The sovereignty framework should serve as a market signal for private companies as much as for public authorities, and the proposal presently gives it almost no means of doing so.

### DIGITAL SME recommendations:

- **Establish SME digitalisation vouchers.** An EU-wide SME Digitalisation Voucher Scheme, restricted to sovereign solutions, would stimulate private-sector demand for homegrown digital companies and strengthen the continent's resilience while accelerating SME productivity across sectors.

- **Activate Article 31 for the private sector.** The Commission should commit to using its delegated powers under Article 31(3) to make sovereignty impact assessments mandatory for entities in sectors of high criticality, so that operators of critical energy, health, transport and financial infrastructure are required to assess their exposure to third-country control.

# 4. Federation of the European cloud market

## CADA proposal

The CADA proposal addresses interoperability only indirectly. Article 41 encourages Union entities and Member States to promote the use of open standards and open-source components when public bodies build their cloud and AI stacks, subject to considerations of functionality, security and total cost. Grand Challenge 2 in Annex I supports the development of end-to-end European cloud stacks, and the Cloud and AI Leadership Initiatives are tasked under Article 4 with fostering open-source software foundations, boosting data availability through open-source middleware, and establishing a catalogue of the European open cloud solutions developed under those initiatives. Beyond these provisions, the proposal contains no obligation, incentive or standardisation mandate directed at interoperability between European cloud providers, and the interoperability requirements applying to data processing services remain those established by the Data Act.

## DIGITAL SME assessment

None of the measures laid out in the proposal addresses why customers stay with non-European platforms, which is rarely the price or quality of storage and compute. Customers stay because a hyperscaler delivers an integrated ecosystem, spanning databases, identity, analytics, monitoring and machine learning services, a marketplace of third-party software, and a supply of integrators trained on that stack.

No single European company can meet the integration and scale requirements of all European customers, and consolidation into a European champion is neither realistic nor desirable. Federation is the realistic alternative, meaning an arrangement in which providers, software vendors and integrators work together in a structured way so that their services can be consumed as a single coherent system. That requires alignment across four building blocks: technical interoperability based on open APIs adopted across IaaS, PaaS and SaaS, common contractual frameworks, accessible joint marketplaces that allow procurement from multiple independent suppliers through a single point of access, and harmonised training and certification so that integrators can work across the ecosystem. Alignment of this kind does not emerge unaided, since incumbents have no interest in becoming composable and smaller providers cannot impose a common layer on their own.

Europe has done this before. The GSM standard succeeded because operators, manufacturers and public authorities committed to a common specification before competing on top of it, formalised in the 1987 Memorandum of Understanding and backed politically by the Commission and Member States. That commitment turned fragmented national telecommunications markets into a continental one, and then into the global standard, and it allowed European industry to build world-leading positions on the layer it created. A comparable commitment is what the European cloud market now needs. Numerous initiatives already work towards parts of this objective on both the public and the private side, and the risk today is duplication rather than absence of effort.

### DIGITAL SME recommendations:

- **Build the technical and commercial foundations of a federated ecosystem.** The CADA should support alignment across the building blocks of federation, namely technical interoperability based on open APIs adopted across IaaS, PaaS and SaaS, common contractual frameworks, accessible joint marketplaces, and harmonised training and certification for the integrators who work across the ecosystem.
- **Make interoperability count in public demand and funding.** Conformity with selected interoperability standards should be a condition for the award of public cloud contracts and for support under the Cloud and AI Leadership Initiatives, so that public spending rewards providers that make themselves composable.
- **Drive convergence and secure political commitment.** The EU should steer existing public and private initiatives towards convergence rather than allow them to duplicate one another, backed by a joint commitment from industry, the Commission and Member States along the lines of the 1987 Memorandum of Understanding that established the GSM standard.

## 5. Data Centre Capacities

### CADA proposal

Article 10 requires every Member State deploying data centre capacity to designate at least one acceleration zone within six months of entry into force. Article 11 sets the conditions inside the zones, requiring Member States to apply defined energy efficiency KPIs and to ensure that resource allocation takes place on fair, reasonable and non-discriminatory terms, without speculative reservation or foreclosure practices capable

of impeding effective competition. Articles 12 and 13 supply the acceleration mechanism by a) giving operators a right to single information point assistance across the full project lifecycle with a dedicated SME channel, b) granting projects in the zones automatic strategic project status under the forthcoming environmental assessment regulation, and c) requiring Member States to issue an aggregated baseline permit for each zone, subject to a 12-month permit-granting deadline. Article 14 allows the Commission to designate individual data centre projects outside of acceleration zonesas strategic through open calls where they meet certain innovation criteria or address a capacity shortage.

## DIGITAL SME assessment

Title III addresses a pressing bottleneck. Permitting delays and grid connection queues are among the most cited obstacles to data centre deployment in Europe, and a coordinated designation of zones with aggregated baseline permits and binding deadlines is a credible response. The benefits attached to that designation are substantial, since accelerated grid access, strategic project status and priority treatment in national planning procedures all amount to a transfer of public value and of scarce physical resources. Eligibility for those benefits is currently blind to who controls the project. Nothing in the proposal links the advantages to any sovereignty criterion, with the result that European regulatory capacity and constrained grid capacity could be used to accelerate infrastructure that deepens the dependencies the Regulation exists to reduce.

The same concern applies to who can realistically access the zones. Article 11 already requires resource allocation on fair, reasonable and non-discriminatory terms and prohibits speculative reservation and foreclosure, which is the right principle. It is accompanied by no allocation methodology, no enforcement mechanism and no reserved share for smaller operators. Grid capacity within a zone is finite and rivalrous, so in the absence of an allocation rule the advantage falls to whoever can reserve connections earliest and hold them longest, which in practice means operators with the balance sheet to carry unused capacity. A framework designed to expand European capacity should not, through the sequencing of access alone, concentrate that capacity in the hands of the largest incumbents.

### DIGITAL SME recommendations:

- **European control as a condition for acceleration zone benefits and strategic project designation.** Eligibility for the advantages under Articles 12 and 13, and for designation as a strategic project under Article 14, should be conditional on the project operator not being subject to the control of a third country or of a legal entity established in a third country, applying the third-country control criterion already set out in Annex II and the corresponding audit evidence in Annex III. In practice, the benefits attached to these mechanisms should go in priority to cloud providers reaching at least Level 3 assurance.

- SME priority access to acceleration areas. The fair, reasonable and non-discriminatory allocation principle in Article 11 should be operationalised through a defined allocation methodology, enforceable limits on speculative capacity reservation, and a reserved share of capacity within each zone for SMEs.

## 6. EuroCloud Federation

### CADA proposal

The CADA proposal establishes the European public sector cloud federation, or EuroCloud Federation, under Article 34, open to Union entities and public sector bodies on a voluntary basis and supported by a Commission-operated platform providing a catalogue of available services and an orchestration layer for exchanging computing, storage and network resources. Article 35 sets the conditions for sharing services within the federation, requiring the sharing entity to own the hardware directly or through an intermediate legal entity over which it exercises control, to put in place appropriate technical, operational and organisational measures, and to demonstrate compliance to the Commission before sharing begins. Fees between members are limited to cost recovery and do not constitute a pecuniary interest within the meaning of the public procurement rules.

### DIGITAL SME assessment

The EuroCloud Federation is a welcome mechanism to pool underused public sector capacity and reduce fragmentation across national administrations. Its design nonetheless closes it to the European industry it should be supporting, since the hardware ownership and control conditions in Article 35(1) apply the in-house logic of public procurement law and exclude private providers from the sharing side entirely, including European SMEs already supplying the same administrations under contract.

That construction creates a second problem. The procurement obligations in Article 30 attach to contracting authorities that procure cloud computing services, whereas a using entity obtains services through the federation without procuring them. Nothing in Articles 34 to 36 imposes any assurance level requirement on shared services, and the conditions in Article 35 concern hardware ownership and technical measures rather than sovereignty. A federation intended to strengthen European capacity should not become the route through which services circulate between administrations without meeting the standard those same administrations would have to apply had they bought them.

### DIGITAL SME recommendations:

- **Open access to trusted private entities**. The conditions in Article 35(1) should be revised to create clear pathways for European private providers, federated SME ecosystems and trusted industry actors to contribute to federated value chains and benefit from the resulting market opportunities.
- **Establish a sovereignty floor for the federation.** Services shared through the federation should be subject to the same assurance level obligations that would apply if the using entity procured them directly, determined by the risk assessment under Article 29.

## 7. Open Source and the EU Solutions Catalogue

### CADA proposal

Article 41 provides that Union entities and Member States shall encourage public bodies to use and reuse open standards and open-source components when building their cloud and AI stacks, taking into account functionalities, security, total cost of ownership and other relevant criteria. Articles 42 and 43 establish the EU Open Source Solutions Catalogue, obliging public bodies that release software they own under an open-source licence to do so through a repository connected to the catalogue, maintained by the Commission on the Interoperable Europe portal. Article 44 establishes a network of Open Source Programme Offices, and Article 22 requires the Commission to maintain a central repository of cloud services recognised under the sovereignty framework.

### DIGITAL SME assessment

DIGITAL SME supports the attention given to open source in the proposal, since open-source components underpin a substantial share of the European cloud and AI stack and the reuse of publicly funded software reduces duplication and lock-in. However, two gaps remain.

Firstly, both the EU Open Source Solutions Catalogue and the catalogue foreseen under Article 4 cover software developed by or for the public sector, and neither gives a public buyer a way to discover the breadth of European solutions available on the market. The instrument closest to that function is the central repository under Article 22, whose role is administrative and is not developed into a tool supporting discovery or procurement. European providers remain largely invisible to the buyers the framework is meant to direct towards them, and this applies equally to open-source projects and to the proprietary and hybrid offerings that make up the majority of the European market.

Secondly, the open-source components on which European sovereignty depends are also maintained by a small and structurally underfunded community, in which European SMEs, foundations and individual maintainers carry a disproportionate share of the work. Encouraging public bodies to build on open source without addressing the sustainability of what they build on transfers risk onto actors with no capacity to absorb it.

### DIGITAL SME recommendations:

- **Adopt an inclusive approach covering all European solutions** to better reflect the diversity of the market and maximise the catalogue's impact. The Tech Sovereignty Catalogue could serve as a basis for developing such an inclusive framework.
- **Fund the maintenance of critical open-source components.** The Cloud and AI Leadership Initiatives should provide sustained funding for the maintenance and security of the open-source components underpinning the European stack, channelled so that it reaches the European SMEs, foundations and maintainers that carry this work.

## 8. Conclusion

The Cloud and AI Development Act establishes a credible framework for building European capacity in cloud and AI. Auditable levels of sovereignty, binding procurement obligations tied to those levels, faster permitting for data centre capacity and a federation to pool public sector resources together represent the most substantial response the EU has yet made to a structural dependency affecting more than 80% of its digital infrastructure. DIGITAL SME supports this direction. The recommendations set out above are not objections to the approach but conditions for making it work.

A first set of conditions converge on a single point: the framework's value depends on whether its thresholds mean in practice what they promise on paper. Else, if Level 3 can be reached through political designation or corporate restructuring, if audits are conducted to a standard that varies across 27 Member States, if certification is priced beyond the reach of the companies it was designed to support, and if the federation and the acceleration zones operate outside the sovereignty criteria applied everywhere else, then the framework will formalise existing dependencies rather than reduce them.

The second condition concerns demand. Investment in chips, cloud infrastructure, AI capacity and data centres is necessary, but it will not by itself produce competitive European providers. Capacity built without a market to absorb it does not translate into scale, and public procurement alone, covering a modest share of European cloud spending, cannot generate the volume required. Europe needs demand that is broad, coordinated and sustained across both the public and the private sector, supported by instruments such as SME digitalisation vouchers, by a measurable trajectory for public administrations, and by extending sovereignty assessment to the critical private-sector operators the Regulation already contemplates.

The co-legislators now have the opportunity to convert a well-designed framework into a functioning market. DIGITAL SME stands ready to contribute to that work on behalf of the digital SMEs it represents across Europe.

## ABOUT DIGITAL SME

The European Digital SME Alliance (DIGITAL SME) is the largest network of small and medium-sized enterprises (SMEs) in the ICT sector in Europe, connecting more than 45,000 digital SMEs. The Alliance is the joint effort of 30 national and regional SME associations from EU Member States and neighbouring countries to put digital SMEs at the centre of the EU agenda.