Brussels, October 2026

The Cloud and AI Development Act (CADA) - Salesforce Position Paper

Salesforce welcomes the opportunity to respond to the European Commission's public consultation on the Cloud and AI Development Act (CADA). We support the Commission's overall objective of promoting the uptake of AI and cloud services across the EU, and welcome CADA's risk-based design as the right foundation to achieve this, consistent with the EU AI Act, the Apply AI Strategy and the 2030 Digital Decade targets. A framework that scales obligations to actual risk, rather than applying uniform rules regardless of context, is the correct starting point for growing safe and trusted adoption of cloud and AI services in the public sector and beyond. Well-designed regulation that promotes meaningful technical and operational controls, and fosters resilience, choice and innovation, can accelerate Europe’s trajectory to becoming a global leader in AI.

Salesforce is a global leader in cloud-based, AI-enabled customer relationship management (CRM) software, offering Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) solutions to enterprises and public sector organisations across the EU. We have operated in the EU for 26 years and maintain offices in 12 Member States.

We offer these comments to supplement the perspectives already shared in our response to the previous call for evidence, including areas where we believe CADA's current drafting would benefit from further refinement. Given that the vast majority of enterprise cloud and AI management applications, including core SaaS productivity, customer engagement, and business platform services, fall within the scope of Union Assurance Level 1 (UAL 1), our feedback focuses specifically on ensuring this entry tier is operational, scalable, and effective.

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

Harmonization, modernization, and simplification

Salesforce supports the European Commission's vision under CADA to build a unified, competitive, and resilient digital single market.

In particular, we welcome the draft regulation's commitment to harmonizing accreditation, assessment, and certification processes across Member States. A patchwork of divergent national approaches to cloud trust and sovereignty risks fragmenting the internal market and slowing public sector digital transformation. CADA's Union assurance levels (UAL), and the mutual recognition mechanism that lets a positively concluded EU statement of conformity or audit opinion be recognized across all Member States, directly address this.

We also welcome the harmonized rules on auditing organizations' independence and audit-opinion formats, and the creation of a central repository of recognized Union-assured services, which together ensure that "Union assurance" carries the same evidentiary weight wherever it is granted, giving public sector procurers in every Member State a common, trusted reference point when assessing enterprise cloud and AI vendors.

We encourage the Commission to maintain this baseline of maximum harmonization throughout the legislative process, including through centrally coordinated guidance mapping assurance levels to data sensitivity categories, to prevent divergent national interpretations from creating new barriers to adoption.

Furthermore, we commend the Commission's focus on modernizing, digitizing and simplifying public procurement mechanisms. A streamlined, transparent procurement process ensures public administrations can seamlessly, timely, and cost-efficiently access state-of-the-art enterprise cloud capabilities and trustworthy AI, ultimately driving better public service delivery for citizens and accelerating digital transformation across Europe's public sector.

AI Agents as Part of the Cloud & AI Leadership Initiatives

Salesforce commends the Commission for including targeted support for advanced AI systems under CADA's Cloud and AI Leadership Initiatives, including Grand Challenge 7 on an AI Agents Platform. European competitiveness depends on accelerating cutting-edge AI adoption across key sectors. The emergence of AI agents, which are autonomous systems capable of

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

reasoning, planning, and executing multi-step tasks across enterprise software, represents the next frontier in digital transformation and workplace productivity.

Deploying AI agents at scale requires seamless integration with reliable cloud infrastructure, rich enterprise data pipelines, and robust trust frameworks. We particularly welcome Grand Challenge 7's focus on exploring technological paradigms that enable multiple AI agents to collaborate effectively, and on developing resilient, secure middleware for deploying autonomous agents at scale. This is complemented by the need for targeted testing and experimentation methodologies for these systems, which is essential: as agents move from single-task assistants to coordinated systems performing complex, multi-step work, transparent orchestration and rigorous testing before and during deployment remain an active area of development across the industry, and are what will ultimately earn the trust of public administrations and citizens alike.

By partnering with cloud platform providers to facilitate real-world testing and evaluation, the EU can bridge R&D directly with commercial deployment. We urge the Commission to build the AI Agents Platform on open, interoperable standards that prevent fragmentation and allow European businesses to adopt agentic AI securely, and to develop its testing methodologies and orchestration standards in close coordination with industry actors already deploying agents at scale.

To maximize the impact and interoperability of these Grand Challenge initiatives, we encourage the Commission to design the resulting orchestration standards and testing frameworks openly, so that trusted digital providers operating under the Union assurance framework can build on and interoperate with them, regardless of where providers are established. European competitiveness thrives in an ecosystem driven by technical merit and open standards. We further recommend that the Union assurance framework explicitly recognize existing international standards, such as ISO/IEC 42001 for AI management systems, as valid evidence of a provider's AI governance and trustworthiness when assessing conformity, avoiding duplicative certification burdens for providers already operating under recognized global frameworks. An orchestration framework built this way would let public and private entities alike combine the best available cloud and AI tools, while remaining fully consistent with the Union assurance criteria that govern which providers may handle sensitive workloads at each level.

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

Metadata and telemetry localisation in Union Assurance Level 1

The comments below focus on Union Assurance Level 1 (UAL 1), which the impact assessment itself recognises will apply to the great majority of public sector cloud use cases across the Union — from municipal services and citizen-facing portals to routine administrative systems. Given the scale of this level and its intended role as the entry point for the broadest range of public sector digital transformation, we believe it merits particular attention to ensure its requirements are proportionate to the risk profiles it actually covers.

Metadata and telemetry data, including service usage logs, performance diagnostics, error reports, and system monitoring data, play a critical operational role for cloud providers. They are essential inputs for maintaining service quality, detecting and responding to security incidents, optimising performance, and providing customer support. Much of this data is highly technical and low-sensitivity.

According to UAL 1 as currently drafted, all public sector use cases will have to comply with strict geographical restrictions for the storage and processing of metadata and telemetry data. However, applying a hard geographic restriction for metadata and telemetry data at this scale, and across such a wide range of risk profiles and data sensitivity levels goes against the EU law's foundational principle of proportionality. UAL 1 encompasses an extraordinarily heterogeneous range of public sector entities: municipal libraries, local citizen services portals, regional health information websites, and minor administrative tools sit alongside more sensitive applications. Imposing identical obligations, including exclusive EU-based storage and processing of metadata and telemetry, on all of them treats a municipal library service and a defence contractor as equivalent, imposing the same infrastructure costs and operational constraints on both, regardless of the actual risk and sensitivity of the data involved.

This is the opposite of what a risk-calibrated regulatory framework is designed to achieve, and goes against CADA's own tiered design logic. The purpose of a multi-level sovereignty framework should be to reserve the most demanding requirements for the most sensitive use cases. Applying hard geographic constraints at the lowest level, to workloads that, by the framework's own classification, pose the lowest risk, inverts this logic entirely.

These localisation requirements also create a risk of increased costs for public sector organisations. To meet the CADA requirements on metadata and telemetry data, cloud providers would need to deploy, maintain, and operate entirely separate telemetry and

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

monitoring infrastructure within the EU, even where the underlying service data is already subject to EU residency under existing contractual or regulatory obligations. As a result, compliance costs would increase, being ultimately borne by public sector procurers, in particular smaller public administrations who will make up the majority of UAL 1 customers. This will translate directly into higher costs for digital services (and increased public spending in a context of state and local government budget constraints), constrained procurement choices, and slower digital transformation.

Furthermore, CADA's proposed broad approach to the localization of metadata and telemetry data at UAL 1 would be materially broader than the risk-based approaches found in comparable international government cloud frameworks. These frameworks generally govern telemetry and metadata security based on impact severity, rather than imposing uniform geographic restrictions across all operational information. For instance, US framework FedRAMP draws the line based on system impact: while metadata that directly impacts system security controls (such as IAM configurations or vulnerability scan data) is protected within the defined authorization boundary, general service telemetry, diagnostic metrics, and platform performance logs may be treated more flexibly.

Instead of hard restrictions on the geographic location of metadata and telemetry data, CADA UAL 1 should leverage technical safeguards, primarily robust encryption and customer-configurable access policies and key control, to mitigate unauthorized access risks. Independent research confirms that data security is determined by *how* data is protected, not *where* it is stored. This approach aligns directly with leading EU publications, including the following:

- ENISA's Cloud Security Guide for SMEs states that "security depends far more on the organizational and technical security measures implemented by the cloud service provider than on where data is physically stored".
- The EDPB Recommendations 01/2020 on supplementary measures for international transfers highlights that when addressing risks of foreign surveillance, technical safeguards, such as state-of-the-art encryption where key management remains under EU control, serve as the primary effective mechanism to prevent unauthorized access.

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

Therefore, we recommend that mandatory geographic localisation for service-generated metadata and operational telemetry be removed from UAL 1. This removal will also ensure coherence with the EU's existing regulatory framework. As data controller under GDPR for this type of data, cloud service providers require operational autonomy over this data to fulfill direct statutory obligations under GDPR Article 32 (Security of Processing) and the NIS2 Directive. Instead, CADA should require cloud service providers to implement robust technical and organisational safeguards to protect metadata and telemetry data against unauthorized access.

The scope of "subcontractors"

Salesforce supports CADA's risk-based approach to supply chain security and third-party risk management. In particular, we welcome the draft regulation's definition in Annex III UAL 1 point 1.2 restricting "subcontractors" to entities that have a *direct* contractual relationship with the cloud or AI service provider and that contribute to the provision and the delivery of the service.

In today's digital economy, enterprise cloud architectures and multi-modal AI systems rely on dynamic, multi-layered technology supply chains involving hardware manufacturers, network operators, specialist software components, and infrastructure partners. Requiring a direct contractual relationship provides a clear, enforceable boundary for audit rights, security reporting, and compliance accountability, that can be easily verified against actual contracts, and then, as per traditional contracting structure, flowed down through the chain.

However, as currently drafted, the definition captures *any* third party that "contributes to the provision and delivery of the service" under a direct contract, without any threshold for how significant that contribution needs to be. Read literally, this could capture vendors with no meaningful connection to the service's security, resilience, or sovereignty profile, e.g. office facilities services, catering, or general administrative vendors. That is clearly not the intended target of a cloud and AI sovereignty framework. Therefore, we urge the Commission to refine the text by explicitly specifying that obligations apply to subcontractors involved in the *material* provision of the covered cloud or AI service. Without a materiality threshold, a literal reading of the provision could sweep in non-ICT operational services (such as facility maintenance, catering, or physical site security) that do not touch data processing or software delivery layers. This clarification would also further align CADA's scope with the materiality principles established under the Digital Operational Resilience Act (DORA), focusing regulatory oversight

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

on critical ICT supply chain risks, while maintaining administrative proportionality for both providers and public procurers.

Infrastructure and assets localization

To ensure UAL 1 fulfills its role as an accessible, baseline assurance level for everyday public sector operations, its requirements must reflect the operational mechanics of modern enterprise software and cloud platforms. UAL 1, point (b) requires that “the infrastructure and assets of the cloud computing service provider, including those of its subcontractors which are involved in the provision of the service, are located in the Union.”

Global providers rely on globally distributed functions that cannot realistically be confined to EU territory without a wholesale re-architecture of how cloud services are built and operated. These include, at minimum:

- Technical operations: the engineering, patching, and maintenance functions that keep a global multi-tenant service running are typically organized around global operational teams, and are not siloed by region.
- Log and diagnostic data: much of the log data generated in operating and securing a service is processed through global tooling and pipelines.
- Customer support data: support functions frequently draw on globally-distributed teams and systems to provide continuous, follow-the-sun service coverage.
- Underlying hardware, firmware, and network/backbone dependencies: the deeper layers of global cloud infrastructure (chip and hardware suppliers, network backbone providers, and similar dependencies) are not sourced on a region-by-region basis by any major provider today.

No major cloud or AI provider, whether headquartered in the EU or elsewhere, currently operates on a fully self-contained, EU-only technology and operational stack, and building one would require duplicating global infrastructure, tooling, and staffing models specifically for the EU market.

The practical consequence is that UAL 1, point (b), as currently worded, sets a bar that would be barely possible to meet for any global provider, including for providers actively investing in EU sovereignty offerings. A requirement that cannot realistically be satisfied will either remove the option of compliance, which risks narrowing the pool of providers able to serve UAL 1 public sector customers, or force superficial compliance claims that do not reflect genuine operational reality.

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

Therefore, we recommend the Commission recalibrate point (b) to focus on outcomes that are both meaningful and achievable, including EU data residency and EU-controlled access and key management, rather than an unqualified requirement that all infrastructure and assets, including those of subcontractors, be physically located in the Union. This would allow the framework to meaningfully advance its sovereignty objectives without setting a compliance bar that excludes the very providers the EU public sector currently relies on for both existing and future services.

Conclusion

Salesforce is a committed partner to the European Commission in building a trusted, competitive, and sovereign cloud ecosystem in Europe. We believe CADA can be a genuinely transformative piece of legislation, but only if it is calibrated carefully to the risk profile of the use cases it governs, technically coherent across cloud service models, and aligned with the EU's foundational principles of proportionality and competitiveness.

Salesforce remains available to engage in further technical dialogue with the Commission and looks forward to contributing constructively to the finalisation of CADA.

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce