



Google Sweden AB
Kungsbron 2, 111 22 Stockholm, Sweden

Finansdepartementet

fi.remissvar@regeringskansliet.se

fi.ofa.dis.remisser@regeringskansliet.se

Datum: 2 okt. 2026

Diarienummer: Fi2026/01676

Googles remissvar avseende Europeiska Kommissionens förslag till förordning om utveckling av moln och AI KOM(2026)502

Inledning

Google välkomnar möjligheten att bidra med synpunkter till den svenska regeringens ställningstagande gällande Europeiska kommissionens förslag till lagstiftningsakt om moln- och AI-utveckling (*Cloud and AI Development Act*, CADA). I linje med vårt långvariga engagemang och våra investeringar för att leverera suverän molntechnologi och datainfrastruktur till Europa, stödjer Google syftet bakom CADA: att bygga en konkurrenskraftig, innovativ, motståndskraftig och tekniskt suverän europeisk digital ekonomi.

Vi hoppas med vårt bidrag till diskussionen om CADA säkerställa ett ramverk som uppnår dessa mål genom ett fortsatt nära partnerskap mellan betrodda globala ledare inom AI, cybersäkerhet, suveräna teknologier och datainfrastruktur. Det är vår övertygelse att suveränitet och tillväxt inte står i konflikt med varandra, utan både kan och bör uppnås parallellt för Sveriges och Europas framtida konkurrenskraft, välbefinnande och säkerhet. För samtidigt som Sverige och Europa har en enorm tillväxtpotential inom AI (1 200 miljarder euro) möter vi också ökande cybersäkerhetshot.

Google välkomnar den svenska regeringens långvariga arbete och stöd för fortsatt globala värdekedjor och för att upprätthålla det transatlantiska samarbetet. Den svenska regeringens förespråkande – tillsammans med den bredare D9-gruppen av länder – för ett öppet förhållningssätt till digital suveränitet, förankrat i samarbetsandan *"Made with Europe"*, är avgörande för att säkerställa en proportionerlig ansats i CADA.

Nedan presenterar vi våra viktigaste prioriteringar och politiska ståndpunkter kring CADA, och vi välkomnar möjligheten att fokusera på särskilda intresse- eller orosområden när den inledande remissrundan har avslutats.



Google Sweden AB
Kungsbron 2, 111 22 Stockholm, Sweden

Våra centrala prioriteringar gällande CADA

- **Skydda nationell suveränitet:** Medlemsstaternas eget bestämmande inom försvar och nationell säkerhet måste värnas; räckvidden i bilaga II riskerar i dagsläget att urholka detta.
- **Undvik överreglering av den privata sektorn:** Offentliga riskbedömningar bör inte per automatik överföras på privata NIS2-entiteter.
- **Motverka protektionism:** Lokaliseringskraven och tredjelandskontrollerna (artikel 18 och bilaga II) riskerar att leda till en protektionistisk ordning snarare än öppen innovation.
- **Skapa ett pragmatiskt granskningsramverk:** Kraven på revision och granskning måste vara praktiskt genomförbara i verkligheten.
- **Säkra cyberförsvaret genom fri data för hotbildsanalys:**
 - Den svenska ståndpunkten bör tydligt **skilja mellan kundinnehåll och säkerhetsrelaterad telemetri/metadata**.
 - Krav på lokal lagring av telemetri försvagar EU:s motståndskraft. Global dataanalys är tekniskt outhållbar för att i realtid upptäcka attackmönster och neutralisera gränsöverskridande cyberhot innan de når mål i Europa.

Sara Övreby
Samhällspolitisk chef, Google Sverige



Google Sweden AB
Kungsbron 2, 111 22 Stockholm, Sweden

General Approach: Competitiveness, Simplification, and Market-Based Growth

Regulatory Simplification and Proportionality

CADA must support regulatory simplification, technology neutrality, and proportionality. To fully deliver on this, we encourage Member States to ensure that new legislation avoids duplicating existing obligations under the Data Act, NIS2, GDPR, and the Cybersecurity Act, thereby safeguarding European competitiveness and AI adoption.

Market-Based Development of Cloud Infrastructure

Cloud infrastructure and computing capacity should be developed as much as possible through market-based mechanisms, focusing public funding (RDI, growth financing, innovative procurement) on scalability and open competition. We support a market-driven approach. Commercial investment, guided by transparent energy/grid frameworks and customer demand, offers the most efficient path to scaling resilient European computing capacity.

Pillar II: Data Centers, Permitting & Acceleration Zones (Articles 10–15)

Voluntary Designation of Acceleration Zones (Article 10)

We welcome Sweden's attention to Data Center Acceleration Zones. Grid capacity allocation should be based strictly on electricity market rules without unjustifiably displacing other investments or allowing speculative reservations.

Zones should function as a facilitative option, not a precondition for investment: development outside designated zones must remain flexible, non-discriminatory and unencumbered, and must not be slowed down or made subject to additional regulatory bottlenecks by virtue of falling outside a zone boundary.

Where zones are designated, they should be selected on the basis of compute demand, connectivity and available grid capacity rather than geographic quotas. Sustainability requirements should be anchored to the EU Rating Scheme, with flexibility for local environmental, climate, water and heat-network conditions.

We would encourage Sweden to use zoning proactively to build economic ecosystems around data centre campuses. Setting aside pre-zoned adjacent industrial land allows auxiliary businesses — greenhouses, vertical farming, aquaculture and district heating



Google Sweden AB
Kungsbron 2, 111 22 Stockholm, Sweden

networks — to connect directly to data centre waste heat. This turns zoning from a permitting hurdle into a regional growth instrument and is, in our experience, the single most effective way to secure durable local support for large-scale investment.

Google Cloud suggests a flexible approach aligning acceleration zone designation with existing clean energy availability and grid infrastructure rather than top-down geographic zoning. At the same time, mature grid connection requests outside designated zones should retain enforceable timelines and cannot have contracted capacity delayed, frozen, or reallocated due to non-zone status.

Additionally, to avoid regulatory fragmentation, any sustainability requirements for data centers should be anchored to the EU Rating Scheme, allowing for flexibility for localized environmental, climate, water and heat network conditions.

Pillar III: Cloud Sovereignty, Assurance Levels & Certification (Articles 16–28)

Personnel Nationality Requirements (Articles 16, 29 & Annex II)

In general, we believe trustworthiness is best established through objective background checks and voluntary sliding scale controls, as opposed to hard and binary nationality/EU controls.

We believe the personnel nationality restrictions at assurance levels 3 and 4 are a blunt and overly restrictive approach. Google Cloud has provided a menu of options for personnel and operational localisation depending on the needs of individual customers and regulatory contexts. We encourage the Commission to set guidelines and allow regulated entities to decide their own personnel needs based on particular operational contexts. For instance, an entity may in some contexts want to maintain a 24/7/365 follow the sun security or customer service model benefiting from globally located personnel. Restricting staff by citizenship hampers access to global technical expertise and reduces security effectiveness without enhancing trust.

The unrestricted references under CADA Annex II to any subcontractor personnel involved in the provision of the cloud services (must be EU citizens) would mean that subcontractor personnel cannot provide cloud services even if those personnel are located - and have a right to work - within the EU. As CSPs and their subcontractors often draw on a global talent pool even within their European operations, this requirement is likely to significantly hinder CSPs ability to provide critical national security services within UAL 3 and 4. It may also result in cost increases and impact Europe's competitiveness as the most qualified personnel are unable to be involved in the provision of cloud services.



Google Sweden AB
Kungsbron 2, 111 22 Stockholm, Sweden

Audit, Certification, and Workable Compliance (Articles 19–21)

Art. 20 (4) (a) attempts to define conflicts of interests, outlining reasons to prevent an audit firm from qualifying for service delivery to the provider. (4) (a) ii. is introducing a 10-year blocking period for cooperation with the firm in question. Under such conditions, qualified audit firms will be automatically disqualified for 10 years after the first use. Additionally, (a) i. Introduces a very broad ban on non-audit service provision. Major firms provide a wide array of tax, consulting, and local compliance services globally. Since the restriction under i. extends to any connected legal person, already a minor engagement with a provider's affiliate anywhere in the world disqualifies the entire global audit network from bidding on an audit service delivery. The 10-year retroactive auditor rotation rule could effectively require a new auditing firm every single year. Under such an interpretation, since CADA audits are annual, providers such as Google Cloud would need a stable of ten entirely separate, highly qualified firms to cycle through over a rolling 10-year period. This "cooling-off period" has no explained policy rationale. At the same time, CADA Art. 20 (4) introduces regulatory fragmentation, by selecting a diverging approach from other EU regulation: *The DSA only prevents using an auditor for more than 10 consecutive years, allowing the same firm to be reused year after year up to that limit.*

Given the existing market for auditing firms, finding ten separate, competent audit firms with the scale and capacity to audit hyperscale cloud environments is near-impossible. Combined with the other restrictions (e.g., on non-audit services), the pool is effectively reduced to zero. Such prescriptive and unworkable auditor eligibility rules will disqualify virtually every competent auditor in the market and will mean CSPs cannot certify their services, creating an artificial bottleneck that halts the EU public sector's cloud adoption.

Adjust requirements for subcontracting to reflect market realities and provide legal clarity

Scope of Subcontracting: What constitutes a subcontractor is left undefined in CADA. This leaves the prospect that CADA's subcontracting requirements apply to any contractors instructed, directly or indirectly, by the Cloud Service Provider (CSP) to perform and deliver part of the cloud services. Crucially, this means that the applicability of any subcontracting obligations are not clear, proportionate or risk based as they could extend to any subcontractor regardless of what role they play in the provision of the cloud services.

Geographic restrictions: All UALs mandate that subcontractors' infrastructure, assets, personnel, and corporate establishment which are involved in the provision of the cloud services are located in the EU. UALs 3 and 4 also require EU citizenship for subcontractor personnel.

Hyperscalers' and their subcontractors' infrastructure, assets and personnel are often



Google Sweden AB
Kungsbron 2, 111 22 Stockholm, Sweden

distributed globally. In practice, this requirement is unworkable, will be profoundly disruptive to the supply of cloud technology within Europe and will preclude many CSPs – including those based in Europe who use global subcontractors – from offering their services at all under UALs, 2, 3 and 4.

Moreover, UALs 2, 3 and 4 contain a separate requirement that technical and operational support or assistance (including “sub-outsourcing arrangements”) are “initiated and performed exclusively within the Union”. It is normal practice for CSPs to have support personnel globally, particularly when providing follow-the-sun support 24x7x365. Restricting the provision of support by personnel “exclusively” based in the EU may raise costs and degrade performance by preventing support queries from being addressed in the most efficient manner by the personnel best placed and knowledgeable to address technical issues.

Overall, the breadth of CADA’s subcontracting requirements is likely to prevent or significantly impede CSPs from offering their services under all UALs and, in particular, UALs 2, 3 and 4. In many cases, compliance with CADA’s requirements is not practicable; in other cases, in order to comply, costs may increase and access to best-in-class services and support may need to be restricted within Europe.

Third-Country Recognition

The blanket restrictions on third-country market access under Article 18 present severe risks of market isolation for Europe and we strongly encourage Member States to seek to remove these provisions. We recommend **reversing the mechanism in Article 18 so that third-country association is presumed by default**, accompanied by clearly defined backstop powers to impose restrictions against a prescribed list of high-risk entities or jurisdictions in exceptional cases, such as verified threats to national security.

While we understand the European ambition to consider the impact of adequacy and government measures on resilience and business continuity of consumed cloud services for the EU public sector, we urge Member States to avoid an overly discriminatory approach. Third-country recognition could be aligned with the objective and evidence-based designation framework established under the Industrial Accelerator Act (IAA). Here, origin and market access are anchored in standard international frameworks—such as free trade agreements, customs unions, or the WTO Government Procurement Agreement (GPA)—providing a clear and objective basis for global partners to navigate.

Data Localisation: Security Telemetry and Metadata

We call attention to the unintended cybersecurity risk that the provisions under CADA Annex II 1.1 c), 2.1c), 3.1c) and 4.1c) for mandatory localisation of telemetry and metadata to Europe would introduce for the European public sector.



Google Sweden AB
Kungsbron 2, 111 22 Stockholm, Sweden

These provisions would prevent access to and protection by cutting-edge global cloud security services, including globally sourced threat intelligence data and automated cyber defence. Analyzing global, cross-border metadata and telemetry (including security configurations) is essential to map malicious infrastructure, diagnose threats, automate defensive operations, and quickly patch widespread misconfigurations. This unified visibility is critical to proactively defend EU public sector entities and critical workloads against sophisticated, globally distributed cyber espionage campaigns.

Treating telemetry and metadata in a strictly localized or geo-restricted fashion fractures global visibility and creates dangerous blind spots. Without cross-border visibility, threat researchers are unable to cross-reference local EU attack patterns with global activity to rapidly correlate threat intelligence.

Limiting telemetry to specific regions prevents the rapid tracking, attribution, and disruption necessary to stop highly capable threat actors. Without cross-border visibility, local government systems lose the protection of a worldwide defensive network, inadvertently giving attackers the advantage.

When threat intelligence is siloed, crucial telemetry data cannot be shared globally to mitigate pressing cyber security risks. The most effective way to defend against a large-scale attack (such as a distributed denial-of-service (DDoS) campaign or a zero-day exploit) is to identify the threat signatures globally and drop the malicious traffic as close to the attacker's source as possible. If an attack originates in Asia targeting European infrastructure, a globally integrated telemetry network allows Google to block the threat at the Asian edge nodes. If European telemetry is walled off, the system loses the ability to correlate European traffic patterns with global anomalies. Consequently, malicious traffic must reach European borders before it can be effectively analyzed and mitigated, increasing the risk of infrastructure overwhelm.

Examples

The COLDRIVER Case (Russia-nexus protecting EU Member States): COLDRIVER is a highly-active cyber espionage cluster that frequently targets European member states. In June and July 2026, global telemetry allowed Google to detect early-stage COLDRIVER operations targeting organizations outside the EU. Because Google could analyze these early warning indicators globally, we were able to proactively flag the malicious infrastructure in the global blocklist. This global visibility directly shielded EU member states and public sector bodies from being the next victims, neutralizing the threat before it could move laterally into European networks.

The APT43 Case (North Korea-nexus securing EU regions): In January 2026, Google leveraged global internal telemetry (such as MX routing, tracking pixels, and Password



Google Sweden AB
Kungsbron 2, 111 22 Stockholm, Sweden

Protection) to detect an APT43 spear-phishing campaign initially focused on U.S. targets. This global visibility enabled proactive account takedowns and advanced protection enforcement. By neutralizing the infrastructure early, Google successfully dismantled the threat before the espionage campaign could pivot and expand its operations into the European public sector and critical infrastructure.

We encourage Member States to make representations to the Council to address the cybersecurity risk of these provisions for the European public sector. Considering the already existing commitment of Google Cloud to localisation of customer data, we feel confident that European data confidentiality and control can be delivered without an additional localization requirement for telemetry and metadata.

Pillar IV: Demand-Side Measures, Public Procurement & Scope (Articles 29–40)

Addressing Restrictive Software Licensing and Multi-Cloud Barriers

For European public sector institutions and government administrations, digital sovereignty cannot be achieved through single-vendor dependency or closed legacy monopolies. True technological progress and digital market fairness depend on an open, multi-cloud ecosystem anchored in open standards, data portability, and robust interoperability. Anti-competitive and restrictive legacy software licensing practices penalize customers for deploying software across rival cloud providers, distort competition and enforce artificial vendor lock-in. Independent economic research, for example a study authored by Prof. Frédéric Jenny for the [CISPE Quantification of the Cost of Unfair Software Licensing Study](#), revealed that discriminatory terms—such as restrictive Bring Your Own License (BYOL) rules and punitive price markups of up to 300% to 400% for running legacy software on rival cloud platforms—extract an annual "tax" of over €1 billion on the European economy. These financial penalties severely distort procurement and cloud adoption. By eliminating these unfair licensing constraints and mandating open interoperability across cloud and AI architectures, organizations gain the genuine autonomy to migrate workloads seamlessly, avoid proprietary walled gardens, and select cloud infrastructure based purely on security, performance, cost, and innovation.

Advancing Art. 29 CADA: While we appreciate the Commission's focus on open source, we believe that Art. 29 CADA provides an opportunity to strengthen the open source commitment and anchor explicit considerations of multi-cloud under the public sector procurement approach. Art. 29 (2) and (9) should not only introduce a consideration for multi-vendor or multi-cloud strategy but add a reference to software licensing terms and practices. Member States' risk assessments should explicitly evaluate them and consider



Google Sweden AB
Kungsbron 2, 111 22 Stockholm, Sweden

their risk of creating restrictive vendor lock-in, specifically by imposing unfair financial or technical penalties or limited portability across cloud providers.

Exclusion of Private-Sector NIS2 Entities (Article 31)

We strongly encourage Member States to raise objections to the Commission extending mandatory risk assessments to private NIS2 entities and recommend the deletion of Art. 31 to avoid confusion on the intended scope.

Extending public procurement-style sovereignty restrictions into private commercial markets creates severe economic distortions across Europe's core industries. While CADA is framed primarily around public sector purchasing, Article 31 establishes a direct mechanism through Commission delegated acts (Art. 31(3)) to mandate sovereignty impact assessments and operational mitigation measures for private enterprises operating in critical sectors under NIS2 Annex I (such as banking, energy, transport, health, and digital infrastructure). Extending the localisation and third country restrictions to private European companies' commercial B2B procurement restricts their access to best-in-class global software and AI tools, driving up operational costs and placing European businesses at a significant competitive disadvantage against global peers.

Secondly, this private-sector spillover creates regulatory conflict and duplication with established, risk-based European frameworks. Critical private sectors are already subject to comprehensive, rigorously negotiated legislation designed specifically for operational resilience—most notably the Digital Operational Resilience Act (DORA) for financial services and NIS2 for critical infrastructure. These sectoral regimes focus on objective operational reliability, multi-cloud diversification, and demonstrable technical security controls. Layering additional non-technical criteria on top of DORA and NIS2 creates legal uncertainty and potential jurisdictional conflict between financial/energy regulators and digital authorities..

Cloud-enabled defence innovation to protect Europe

Modern defense operations are software-defined, requiring real-time, global threat intelligence and seamless data exchange across allied networks. In the era of AI and persistent state-sponsored cyber threats, access to commercial hyperscale cloud infrastructure serves as the indispensable digital backbone for national security, democratic institutions, and critical infrastructure. Fragmented, legacy on-premise systems can no longer provide the computational scale, physical redundancy, or continuous software updates required to defend against sophisticated adversaries. Commercial cloud environments deliver deep, built-in resilience—spanning globally redundant terrestrial and subsea fiber networks—while providing defense organizations with cybersecurity capabilities that shift defense from reactive perimeter management to real-time threat detection and autonomous vulnerability remediation.



Google Sweden AB

Kungsbron 2, 111 22 Stockholm, Sweden

Equally vital, access to modern cloud architecture is the prerequisite for allied interoperability. By adopting open-standard, multi-cloud platforms, allied armed forces and public sector bodies can dismantle rigid data silos to seamlessly share cross-domain intelligence. Advanced sovereign controls—such as air-gapped infrastructure and customer-controlled encryption—further guarantee that governments can retain full operational autonomy, regulatory compliance, and data sovereignty without sacrificing access to cutting-edge technology.

An exclusion of US hyperscalers for national defence customers under UAL4 will prevent these vital advantages for European defence and security to materialize. Restricting cloud and AI software development or operations exclusively to EU borders would technically isolate EU forces from non-EU allies (such as the US and UK). Sovereignty in defense is, of course, an essential priority but can and must be achieved through robust technical, cryptographic, and operational controls rather than protectionist geographic isolation.

We encourage Member States to seek the deletion of UAL4, to ensure that access to trusted global partners remains consistent within the NATO Alliance. This allows cooperation with providers on both sides of the transatlantic relationship, leveraging operational modern sovereign architectures provided today.

Avoid regulatory overreach in Article 29(5)

Article 29(5) risks encroaching on national decision-making and Member State discretion regarding public order and critical functions. Granting the Commission unlimited backstop authority creates significant legal uncertainty regarding the supremacy of Member State risk assessments. At a minimum, Art. 29 (5) should outline concrete procedures; safeguards that allow Member States to make a case for their initial risk assessment. In order to secure timely European public sector access to innovation technology, any override procedure should only be considered for high risk scenarios and only applicable where more proportionate actions have been exhausted.