To: Ministry of Justice and Digital Affairs

Subject: AmCham Estonia input on CADA / Tech Sovereignty Package

Date: August 27, 2026

Dear Allan Allmere,

AmCham Estonia Digital Society Committee members would like to share our views on the Tech Sovereignty Package, specifically the proposed Cloud and AI Development Act (CADA). Our members include major international technology companies that are significant investors, employers, and innovation partners in Estonia and across Europe.

AmCham Estonia supports the objectives of strengthening Europe's digital resilience, cybersecurity, technological capacity, and AI competitiveness. These goals are important for Estonia and for Europe's long-term security and economic growth. We welcome the ambition to expand EU data center capacity, foster sustainable computing, and ensure operational continuity of cloud services for the public sector.

However, we are concerned that the current proposal, as drafted, equates sovereignty with corporate nationality rather than with verifiable technical and operational controls. This approach risks limiting European customers' freedom to choose the solutions they need to stay secure, competitive, and innovative. What should matter is whether an organization can keep control of its data, keep critical systems running under pressure, move workloads, and combine services across providers. Only technical design, breadth of services, dedicated partnerships, and independently audited controls and assurances can demonstrate this – not corporate nationality.

For Estonia, this is a critical issue. Estonia's digital success has been built on openness, innovation, and access to best-in-class technologies. If trusted non-EU providers are restricted from serving public sector, critical infrastructure, or other important customers, Estonia may face fewer choices, higher costs, slower innovation, and weaker access to advanced cloud, AI, and cybersecurity capabilities. Estonia's own experience during geopolitical crises has shown that globally distributed cloud infrastructure preserved government continuity precisely when local infrastructure was at risk.

AmCham Estonia is particularly concerned about the following aspects of the proposal:

- The Union Assurance Level (UAL) framework grows progressively more restrictive, culminating at UAL 4 in a requirement for a fully EU-controlled software supply chain that no cloud provider, including European ones, can currently meet. This creates a paradox at the heart of the regulation: **the most critical public sector workloads are precisely those most urgently in need of frontier AI capabilities, advanced cybersecurity tools, and global-scale threat intelligence**.
- The associated third-country regime (Article 18) would not automatically extend eligibility to countries such as the United States, Canada, or the United Kingdom, creating legal uncertainty and deterring investment. Unlike the Chips Act, which extends eligibility to GPA/FTA partners, CADA excludes foreign providers by default with no timeline or obligation on the Commission to decide on exceptions. **Strong technical measures** (customer-managed keys, split-key schemes, zero-knowledge encryption, confidential computing) can effectively mitigate third-country lawful-access risks and should **count towards higher UAL eligibility irrespective of corporate nationality**.
- The risk assessment methodology (Article 29) is entirely delegated to a post-adoption implementing act, and the Commission retains power to override Member State assessments. This removes the ability of contracting authorities to determine how best to mitigate risk, collapsing risk mitigation into a single instrument – mandatory provider selection at a given UAL – with no recognition of multi-cloud strategies, contractual exit plans, or customer-managed encryption as legitimate alternatives. Any Commission decision restricting providers should require ex ante impact assessment from key partners, including trade, competition and innovation effects.
- The broader intention to spill over sovereignty requirements into the private sector, as seen in Article 31(1) and (2) as a whole, combined with the extension mechanism in Article 31(3) without ordinary legislative scrutiny, creates systemic legal uncertainty for regulated industries across the NIS2 Annex I sectors. Additionally, CADA implementation must not retroactively undermine legitimate expectations of investors and service users to avoid chilling future investment and risk with systemic disruptions.

AmCham Estonia encourages Estonia to support an approach based on open sovereignty: strengthening European capabilities while preserving cooperation with trusted global partners. The proportionate response to operational continuity concerns in adverse political scenarios is resilience – not exclusion. Multi-cloud architectures, contractual exit plans, service continuity commitments, and technical controls such as customer-managed encryption keys and zero-access operator architectures provide verifiable protection without restricting technology choice. Risk methodology should give priority to verifiable technical and operational controls over formal ownership or place of establishment as the primary determinant of sovereignty risk.

We respectfully recommend that Estonia advocate for a framework that:

- **introduces periodic review of UAL criteria** to ensure they remain proportionate, technologically neutral and aligned with actual threat developments;
- replaces the UAL 1 criteria that the cloud service provider is established in the Union with a requirement that **infrastructure and asset operators are EU-established and EU-located**, combined with a binding EU legal representative for non-EU providers;
- **removes UAL 4 entirely**, recognizing that defense-specific requirements should remain outside the scope of CADA;
- **eliminates references to subcontractors in Annex II** to prevent disproportionate and impractical disruptions to global supply chains;
- reorients from origin-based restrictions toward outcome-based requirements – defining what a provider must demonstrably deliver (verifiable data control, operational continuity, jurisdictional safeguards, transparency) rather than prescribing who a provider must be;
- ensures the risk assessment methodology is subject to co-legislative scrutiny and includes a rigorous impact assessment before adoption, covering costs to national budgets, effects on innovation, and consistency with the EU's trade commitments under the WTO GPA and bilateral FTAs;
- strengthens Article 29 by obliging Member States to include multi-cloud strategies in public procurement and mandating the review of individual vendor lock-in practices during sovereign risk assessments;
- includes GPA/FTA partners in UAL 3 by default, consistent with the approach taken in the Industrial Accelerator Act and Chips Act, to preserve legal certainty and avoid triggering reciprocal trade restrictions against European companies abroad;
- removes or substantially limits the Commission's power to override Member State sovereignty risk assessment outcomes, preserving national discretion based on local security and digital needs;
- removes Article 31(3) mechanism for extending sovereignty requirements to the private sector without full co-legislative procedure and mandatory public consultation.

AmCham Estonia stands ready to continue the dialogue and provide further technical input on how sovereignty objectives can be achieved without undermining competition, innovation, and the trusted partnerships that underpin Europe's digital security.

Respectfully,

AmCham Digital Society Committee