NON-PAPER BY THE NETHERLANDS
AN INTEGRATED APPROACH FOR THE EU TECH SOVEREIGNTY PACKAGE

The Hague, April 17, 2026

The Netherlands looks forward to the upcoming Tech Sovereignty Package as a whole and considers it a timely and focused opportunity to give the European Union a more coherent response to high-risk strategic dependencies in critical digital technologies. However, at present, the various initiatives risk missing potential synergies. A stronger integrated approach would improve consistency between regulation and industrial policy, including the future European Competitiveness Fund and mobilisation of private capital, and would better support the EU's long-term competitiveness, resilience and ability to act in line with its democratic values and the rule of law.

The Netherlands therefore proposes to frame the package around a common concept: a **Sovereign Tech Stack** explicitly built around a demand-supply loop[1] between the layers of the stack, with open-source as one of the key enablers. This approach recognises that technological sovereignty is not binary, but depends on the interplay across the full tech stack, from materials, hardware and infrastructure to software, data and applications. It also supports the EU in its goal to maintain jurisdiction, control over and protection of its data, information and systems, while reflecting the fact that the EU will often need to combine domestic capability with diversified access to foreign technology and materials. It is important to note that EU (cyber)security and privacy law and regulations should be coherent with this approach: special attention should be given to regulation that prevents the misuse of services on this digital infrastructure by criminal and malicious actors.

The goal for sovereignty in the tech stack should be to have the ability to choose and act autonomously on the world stage and in line with our values, while reaping the benefits of collaboration with global partners as much as possible. To improve its technological sovereignty the EU needs to strengthen its technological capabilities, diversify access to technology through trade relations and supply chain management, and safeguard its regulatory autonomy in technology. This ensures the EU maintains its openness, preserves and creates control points in value chains, mitigates high-risk strategic dependencies, ensures risk-based decision-making, develops human capital for tech, and safeguards European law and values. Open source should be treated as one of the cross-cutting enablers of sovereignty and a supply-demand loop within the tech stack.

Takeaways

The Tech Sovereignty Package should send a clear signal: the EU will build a reinforcing supply-demand loop to support a sovereign tech stack. In this model, sovereign cloud and AI deployment drives demand for trustworthy chips, as well as open technologies and standards, while European innovation feeds back into competitive sovereign digital solutions. Such a coherent approach across AI, cloud, digital infrastructure and semiconductors – combined with open source as a cross-cutting enabler and supported by the strategic use of EU financing instruments such as the future European Competitiveness Fund – will strengthen the EU's competitiveness, resilience and better align digital policy with the Union's values, and freedoms.

[1] a self-reinforcing cycle where stimulation in upper-layer technologies of the tech stack (e.g., Cloud, AI) creates a predictable market for foundational layers (e.g., infrastructure, chips), which in turn provide the essential building blocks for those upper layers to scale and function in a sovereign manner.

Against this backdrop, the Netherlands suggests the following priorities for the package.

A. Cloud & AI Development Act (CADA)

The Cloud & AI Development Act should focus on building a sovereign and sustainable EU cloud and AI ecosystem and infrastructure, while actively creating markets for trustworthy and open technologies. In this sense, the Netherlands supports the earlier non-papers shared by Germany and Denmark. In particular, the Act should:

- establish a common, layered definition of a "sovereign cloud" to prevent sovereignty-washing, improve transparency for commercial buyers and suppliers, reflecting different levels of autonomy, control and jurisdiction: ranging from mid-autonomous, high-autonomous to, ultimately, fully sovereign;
- support a federated EU cloud ecosystem; e.g., through the establishment of EU cloud marketplaces; deliverables of ongoing EU initiatives, such as the 8ra Initiative and the Digital Commons EDIC can work as incubators;
- prioritise support for data centre projects with strategic value, including infrastructure used by governments and other critical users, and ensure that the added value to EU competitiveness, control, resilience, security and privacy and sustainability remains central;
- help streamline the development of strategically important data centre capacity, while keeping national and local governmental and non-governmental players responsible for planning and permitting; e.g. through existing or new digital tools for authentication purposes to facilitate secure and efficient administrative processes;
- use public procurement, standards and certification of cloud and AI solutions to strengthen demand for trustworthy hardware and open-source-based solutions developed in and with Europe[2], with the ability to steer on sovereignty;
- ensure that the highest tiers of sovereign cloud layers contain EU solutions that are interoperable and portable, providing true freedom of choice for end-users.

B. Chips Act II (CAII)

Chips Act II should move beyond a focus on large-scale fabrication and place greater emphasis on demand, especially linked to the high-growth market of cloud and AI. Sovereign EU cloud and AI providers can create demand for trustworthy chips which in turn strengthen the sovereignty of these digital services. The Act should therefore:

- define criteria for trustworthy chips, not only based on core security principles but also on supply-chain transparency, stability, added value and integration to the EU ecosystem.
- support open chip technologies, incl. architectures such as RISC-V, enabling transparency, flexibility and EU participation in chip design and prevent single-vendor lock-in;
- ensure complementarity with open-source hardware and software ecosystems;
- encourage strategic partnerships for access to advanced nodes, while embedding these in a broader EU ecosystem;
- align semiconductor policy with cloud and AI stimulation, ensuring that chips developed or designed in the EU are integrated into EU data centres and AI infrastructure;
- leverage coordinated demand (via CADA and innovative public procurement) as an offtake mechanism to scale trustworthy chip solutions within the EU.

[2] This should be 1) limited to selected core and critical strategic areas; 2) temporary in nature; 3) only used where other instruments fail; 4) inclusive for European partners and 5) respect the EU's international commitments.

C. Open Source Strategy (OSS)

The Open Source Strategy should be strategically woven into the broader Tech Sovereignty Package as one of the key enablers of the supply-demand loop between CAII and CADA as an enabler of sovereignty. Open source enables (i) supply, lowering barriers for market entry allowing EU firms to participate in software and hardware development; (ii) demand, allowing cloud and AI providers to adopt interoperable and substitutable solutions; (iii) governance, through transparency, auditability and verifiability across the tech stack. The strategy should therefore:

- ensure alignment with CADA and CAII so that open standards and components are used where possible across the stack;
- strongly advice Member States to adopt policies that promote the establishment of Open Source Program Offices (OSPOs), that can – among other things – function as intermediaries in open source collaboration (within and between governments and public-private partnerships);
- strengthen public-private cooperation on open-source software, hardware, data interoperability, network connectivity and standards, including through consortia, stewardship models and better mobilisation of private capital;
- emphasise the need for full support of the European Commission for Digital Commons EDIC, where both national and EU authorities have a vital exemplary role to fulfil;
- support the development and maintenance of a secure EU open-source base across both software and hardware layers;
- ensure that public procurement rules enable public authorities to act as launching customers for trusted and open-source solutions.