Response from CNLL to the "European Open Digital Ecosystems" Consultation

Respondent: Conseil National du Logiciel Libre (CNLL)

Subject: Contribution to the European Commission's upcoming Open Source Strategy

Introduction

For over 15 years, the **Conseil National du Logiciel Libre (CNLL)** has served as the representative body for the French Open Source professional ecosystem, speaking on behalf of over 300 innovative SMEs and mid-caps that drive employment, local value creation, and digital independence in France. We view Open Source Software (OSS) not merely as a technical methodology, but as the **strategic imperative for Europe's digital sovereignty and industrial competitiveness.**

Our position, fully aligned with our European partners at **APELL**, is that the era of "laissez-faire" in digital policy is over. While the immediate political mandate for action stems from vulnerabilities to extraterritorial laws and supply chain shocks, the root causes are **systemic**. Europe faces a critical choice: continue to suffer from deep technological dependency and structural economic imbalances—where value is extracted by non-EU hyperscalers rather than reinvested locally—or become an active producer and steward of its own digital infrastructure.

To address these systemic failures, the Commission must transition to a robust **industrial policy** that moves beyond soft encouragement to active market shaping. As detailed in this response, this strategy rests on three fundamental pillars:

1. **A "Risk-Based" Technological Doctrine:** Europe must replace naive openness with a rigorous **Sovereignty Risk Assessment Framework**. Technology adoption must be conditional on legal immunity from extraterritorial jurisdictions, supply chain security, and **enforceable interoperability**, distinguishing between safe digital public goods and captured ecosystems.
2. **A Transformed Public Procurement Strategy:** We advocate for a binding **"Open Source First"** principle combined with a strict **"European Preference"** for service providers, and additional measures (promotion, training…) to ensure that this preference is actually enacted. This must include specific mechanisms (like **Allotment**) to ensure public funding reaches the **creators** of the software (Open Source software vendors / *éditeurs de logiciels libres*) rather than being captured solely by integrators, thereby fixing the broken value chain.
3. **Structural Funding for the Digital Public Goods:** We must operationalize this strategy by leveraging existing assets (Horizon/Digital Europe) while deploying necessary new capabilities: specifically, the establishment of an **EU Sovereign Tech Fund** to secure the maintenance of critical infrastructure (ODBTs) and the mobilization of the **DC-EDIC** as a technical assistance facility to de-risk adoption.

By aligning its regulatory power (procurement) with its investment capacity (funding), Europe can secure its digital future.

A. Current state of the EU open-source sector

1. Strengths and Weaknesses of the EU Open-Source Sector

Strengths: A Sovereign, High-Value Industrial Base

The European open-source ecosystem is characterized by a unique level of industrial maturity in "deep tech" sectors. Unlike the consumer-centric software models often seen elsewhere, European SMEs and mid-caps have established themselves as global leaders in critical infrastructure layers such as Embedded Systems, Industrial IoT, Edge Computing, and Cloud Infrastructure. As detailed in the *Cloud-Edge Alliance Roadmap*, European open-source frameworks are already the operational backbone of Industry 4.0, smart cities, and public utilities across the continent.

Furthermore, the European sector offers a unique "sovereignty value proposition" that non-European competitors cannot match. European open-source software (OSS) naturally aligns with the regulatory requirements of the GDPR and the Data Act by offering full code auditability and options for strict data residency. This capability provides public and private entities with what we call a "sovereignty premium": the ability to guarantee legal immunity from extraterritorial jurisdictions (such as the US CLOUD Act or FISA). This is a competitive advantage that is intrinsic to the European model and critical for strategic autonomy.

Finally, the sector acts as a powerful economic multiplier. Investment in open source generates high returns that remain largely anchored within the EU economy. Unlike the license revenues of non-EU proprietary giants which often flow offshore, the economic value of OSS is captured through high-skilled jobs in R&D, consulting, and integration—jobs that are rooted in local territories and cannot be easily outsourced.

Weaknesses: Asymmetric Value Extraction

Despite these strengths, the European open-source ecosystem faces a critical imbalance in value distribution. While it is home to technically advanced SMEs and micro-enterprises, these actors often lack the financial resources to compete with non-EU tech giants. The problem is not their capability but a **"Strategic Blindness" among European National Champions**. Large European integrators and industrial groups (in sectors like Telco, Defense, and Aerospace) frequently bypass the local ecosystem. Instead of contracting directly with the European SMEs that create and maintain the software, they often prefer to source "Enterprise" distributions or cloud services from US vendors or integrate the Open Source components themselves without contributing financially to the original creators.

This behavior creates a severe economic imbalance. **If European industrial leaders sourced their open-source needs directly from local creators (Vendors/*Éditeurs*), the ecosystem would be self-sustaining.** Instead, the current purchasing behavior of Europe's own champions effectively subsidizes foreign competitors or starves the local R&D base, weakening the very economic fabric they rely on for sovereignty.

2. Main Barriers to Adoption and Maintenance of High-Quality Open Source

The barriers preventing the wider adoption of open source are rarely related to the quality of the software itself. Instead, they are primarily the result of cultural inertia and flawed procurement methodologies.

The "Defensive Buying" Syndrome and Risk Aversion

Public procurement is heavily influenced by a culture of risk aversion. Public buyers often default to large, non-EU proprietary vendors not because they offer superior technology, but due to a perceived sense of safety and habit—the "nobody gets fired for buying the incumbent" syndrome. There are currently insufficient incentives for public procurers to take the perceived "risk" of choosing sovereign, open European solutions, despite the long-term strategic benefits.

Flawed Economic Metrics in Procurement

Tenders are frequently structured around metrics that disadvantage open source. Procurement processes typically focus heavily on the initial license price—which is often zero for OSS—while ignoring the **Total Cost of Ownership (TCO)** over the project's lifecycle. Crucially, they fail to account for **exit costs**. Proprietary solutions often hide massive, unpredictable costs required to migrate away or retrieve data, whereas OSS offers near-zero exit costs and greater long-term flexibility. By ignoring the cost of "lock-in," public tenders skew the market in favor of proprietary vendors.

"Open Washing" and Lack of Enforceable Standards The marketplace is confused by "open washing," where vendors claim openness while retaining control over standards and interoperability. Without strict, **enforceable open standards** that mandate genuine data portability and API neutrality, the theoretical benefits of OSS adoption—such as market fluidity and the ability to switch providers—cannot be realized in practice.

3. Main Barriers to Sustainable Contributions: The Intermediary Value Trap

The most critical threat to the sustainability of the European open-source ecosystem is economic. It stems from a broken value chain where the funding provided by public and private consumers does not reach the producers of the technology.

The "Integrator vs. Creator" Disconnect

The central structural failure in the public sector is that administrations rarely contract directly with the companies that actually produce and maintain open-source software (the *Creators* or *Éditeurs*). Instead, public procurement is dominated by massive framework contracts that favor large Systems Integrators and generalist IT consultancies.

When a public administration deploys an open-source solution, they pay significant sums to these Integrators for deployment, customization, and support. However, these Integrators capture the vast majority of this value. They rarely pass a fair share of the revenue back to the SME Publisher that writes, secures, and maintains the core software product.

This creates a parasitic dynamic: the public sector "consumes" the innovation and stability provided by the Publisher but pays the Integrator. This starves the creators of the software of the recurring revenue needed for R&D, security hardening, and maintenance. It weakens the very supply chain the public sector relies on, turning European OSS Publishers into fragile entities despite the widespread use of their products.

Regulatory Chill and Liability Risks

European SMEs face increasing anxiety regarding legal liability. Well-intentioned regulations, such as initial drafts of the Cyber Resilience Act (CRA), create a climate of uncertainty where smaller players fear that publishing open code could expose them to disproportionate financial penalties if a vulnerability is discovered. This "regulatory chill" discourages the release of innovation, hampers the collaborative model that defines open source, and even prevents European Open Source technologies to be sold on the European market.

The Dual Tragedy of the Commons

Finally, the ecosystem suffers from a "dual tragedy of the commons." On one side, there is under-provision: a chronic lack of resources for the maintenance of critical infrastructure due to the value trap described above. On the other side, there is over-exploitation: an ever-increasing demand from users and corporations who integrate free code into commercial products without reinvesting in the upstream communities. This imbalance leads to security vulnerabilities in critical infrastructure where essential components rely on under-funded, over-stretched individuals and teams.

B. Added value of Open Source Software (OSS) for the European public and private sectors

Our core position is that the added value of open source has shifted. While historically valued primarily for cost reduction (no license fees), its primary value today lies in **strategic risk management**: specifically, the mitigation of geopolitical risk, vendor lock-in risk, and supply chain security risk.

1. Digital Sovereignty and Legal Immunity

The most critical added value for the public sector today is the assurance of **digital sovereignty and legal immunity**. As detailed in the *Cloud-Edge Roadmap*, reliance on non-EU proprietary technology providers exposes European data to extraterritorial jurisdiction, such as the US CLOUD Act or FISA 702. Proprietary software acts as a "black box" where the user cannot verify if data is being exfiltrated or if "backdoors" exist.

Open source provides a unique remediation to this risk through **full auditability**. Because the code is transparent, European administrations can independently verify security claims and host the software on sovereign infrastructure (e.g., SecNumCloud in France) without dependency on the original vendor's cloud. This creates a "sovereignty premium": the ability for an organization to guarantee that its digital infrastructure is subject *only* to European law. This is not merely a technical feature but a prerequisite for the autonomy of European institutions and the protection of industrial secrets.

2. Mitigation of Vendor Lock-in and Exit Costs

For both public and private sectors, the most economically significant factor is the reduction of **vendor lock-in** and the associated **exit costs**. In proprietary models, the cost of migrating away from a vendor (the exit cost) is often prohibitively high due to proprietary data formats, obscure APIs, and licensing traps. This effectively eliminates market competition once a vendor is selected.

Open source radically alters this economic dynamic. By adhering to open standards and allowing access to the source code, OSS enables **interoperability and portability**. An administration using an open-source solution (e.g., for document management or cloud infrastructure) retains the freedom to switch service providers—moving from a global integrator to a local SME, or bringing the service in-house—without losing data or having to rebuild the software stack. This restores the buyer's negotiating power and fosters a competitive service market, as opposed to a rent-seeking license market.

3. Security through Transparency and Supply Chain Resilience

The added value regarding security stems from the principle that **transparency outperforms obscurity**. As noted in the *APELL Feedback* and the *OFE Feasibility Study*, the complexity of modern software supply chains makes vulnerabilities inevitable. In a proprietary model, the user is entirely dependent on the vendor's willingness and timeline to patch a flaw.

In the open-source model, security is a collective endeavor. Vulnerabilities can be identified and remediated by a global community of security researchers, independent auditors, and peer organizations. Furthermore, open source enables the generation of accurate **Software Bills of Materials (SBOMs)**, which are essential for mapping dependencies and managing supply chain risks (a key requirement of the Cyber Resilience Act). This capability allows organizations to proactively manage their risk posture rather than passively trusting a vendor's marketing claims.

4. Permissionless Innovation and Economic Competitiveness

For the private sector, particularly SMEs, the primary added value is **"permissionless innovation."** The European digital economy is built upon open source foundations (Linux, Python, PHP, PostgreSQL, MySQL, etc.). These technologies provide a standardized, high-quality industrial base that companies can leverage instantly without negotiating legal contracts or paying upfront license fees.

This accelerates time-to-market and lowers barriers to entry for European startups. Instead of reinventing the wheel, European companies can focus their R&D budget on high-value vertical applications (the "EuroStack industry") while relying on shared open source building blocks for the infrastructure layer. This collaborative model prevents the duplication of effort and allows European SMEs to compete globally by standing on the shoulders of the open-source ecosystem.

5. Environmental Sustainability and Hardware Longevity

Finally, open source creates significant value in the context of the **Green Deal and circular economy**. Proprietary software often drives "planned obsolescence" by artificially limiting support for older hardware (e.g., Windows 11 hardware requirements rendering hundreds of millions of perfectly functional PCs obsolete).

Open source operating systems and applications are typically much more resource-efficient and can be maintained on older hardware for significantly longer periods. This extends the lifecycle of IT equipment, drastically reducing electronic waste and the carbon footprint associated with manufacturing new devices. For public administrations managing vast fleets of hardware, this represents a massive ecological and financial saving, aligning digital strategy with environmental responsibility.

C. What concrete measures and actions may be taken at EU level to support the development and growth of the EU open-source sector?

We propose in this document 28 concrete measures, while referring to the roadmap "The Open Source Way to EU Digital Sovereignty & Competitiveness" published by the European Alliance for Industrial Data, Edge and Cloud last year for additional propositions. All of these measures stem from discussions conducted during workshops at CNLL, APELL and at the Commission (e.g. "Open Source Beyond 2020" in 2019 and "Open Source Sustainability Workshop" in 2021) over the last 10+ years.

Pillar 1: Technological Strategy & Industrial Sovereignty

Strategic Objective: Move Europe from a posture of "passive consumption" to "active stewardship" of the digital infrastructure. This pillar acknowledges that code is global, but **jurisdiction, governance, and supply chain security are local.**

1. Implement a "Sovereignty Risk Assessment Framework"

Context: A simplistic "Buy European" rule for software code is technically unfeasible (modern software supply chains are global) and potentially counter-productive (cutting Europe off from global innovation like Linux or the Python ecosystem). However, blindly adopting non-EU technology creates unacceptable legal risks.

- **The Proposition:** The Commission must establish a standardized **Risk Assessment Framework** (a "Sovereignty Scorecard") for software components used in critical public infrastructure.
- **Detailed Criteria:**

  - **Extraterritorial Exposure:** Is the software vendor or the foundation controlling the project subject to extraterritorial laws (e.g., US FISA 702, CLOUD Act, Chinese National Intelligence Law) that could compel data access or backdoors?
  - **Export Control Risk:** Is the software subject to export administration regulations (e.g., US EAR) that could allow a foreign government to unilaterally revoke Europe's right to use or update the software (the "kill switch" scenario)?
  - **Governance Autonomy:** If the main vendor disappears or sanctions are imposed, can the project be legally and technically "forked" and maintained by European entities? (This requires *a minima* OSI-compliant licensing + availability of build scripts/documentation).
  - **Supply Chain Auditability:** Does the project provide a complete Software Bill of Materials (SBOM) and reproducible builds to verify no tampering occurred between source code and binary?
  - **Expertise in Europe:** Does a sufficiently robust ecosystem of European developers, vendors and service providers exist that can maintain, patch, and evolve the software? Sovereignty is not just legal ownership of the code; it is the operational capability to intervene on it (Level 3 support) without relying on the original non-EU vendor.
- **Nuance:** High-risk components (e.g., non-EU encryption modules) might be banned for *Critical* systems (Defense, Health) but acceptable for *General* use if mitigated by European support contracts.
- *Sources: CNLL Doctrine on Legal Immunity; Cloud-Edge Alliance Roadmap (Pillar 5 - Governance).*

2. Develop Sector-Specific Reference Architectures

Context: Fragmentation is Europe's weakness. If every Member State builds its own custom "sovereign cloud" or "smart city" stack from scratch, the market remains too small for any European vendor to scale.

- **The Proposition:** The Commission should fund the definition and maintenance of **Open Source Reference Architectures** for critical verticals (Healthcare, Education, Smart Cities, Energy Grids…).
- **Detailed Action:**
  - **Standardization by Code:** Instead of just writing PDF standards, fund the integration of existing European open source components into deployable "Reference Stacks".
  - **Interoperability by Design:** These architectures must mandate specific open APIs for all internal modules, ensuring that components can be swapped (e.g., replacing one chat module with another) to prevent lock-in even within the open stack.
  - **Industrialization:** These architectures serve as the "blueprint." European SMEs and integrators then compete to deploy, host, and maintain these specific stacks for public administrations, creating a unified market demand.
- *Sources: Cloud-Edge Roadmap (Pillar 1); EuroStack (Industrialization).*

3. Secure the Supply Chain via an EU Sovereign Tech Fund (EU-STF)

Context: The "Innovation Trap." Public funding (Horizon Europe) loves "new" features. It rarely funds the unglamorous work of maintaining 15-year-old libraries (like OpenSSL or Log4j) that run the internet. This under-funding creates security holes that threaten European industry.

- **The Proposition:** Establish a dedicated financial instrument (EU-STF), modeled on the German *Sovereign Tech Fund*, with a budget of at least **€350M** over 7 years.
- **Detailed Mechanism:**
  - **Focus on ODBTs:** Funding is strictly restricted to **Open Digital Base Technologies** (foundational libraries, protocols, build tools, kernels). It is *not* for building commercial products.
  - **Direct Procurement of Maintainers:** Unlike grant-based research projects (which are administratively heavy), the EU-STF should use agile procurement to pay maintainers (individuals or non-profits) directly for specific tasks: security audits, refactoring legacy code, writing documentation, and generating SBOMs.

    - **Security as a Public Good:** This acts as a subsidy to the security of the entire European economy, fixing vulnerabilities "upstream" so every European company benefits "downstream."
- *Sources: OFE Feasibility Study; APELL; Cloud-Edge Roadmap (Pillar 4).*

4. Mandate "Enforceable Interoperability"

Context: "Open Washing." Non-EU hyperscalers often claim to support open standards while subtly breaking interoperability (e.g., "embrace, extend, extinguish" tactics) or using "FRAND" (Fair, Reasonable, and Non-Discriminatory) patent terms that are incompatible with Open Source licensing.

- **The Proposition:** Move from "encouraging standards" to **"Enforceable Interoperability"** legislation.
- **Detailed Action:**
    - **Strict Definition (EIFv1):** Mandate that "Open Standard" in public procurement *must* mean: Royalty-Free, specifications publicly available, and no constraints on reuse (making them compatible with, e.g., GPL/MIT/Apache licenses).
    - **Data Portability Rights:** Grant public administrations a legal right to **bulk data extraction** in a standard format (with metadata) within a set timeframe (e.g., 48 hours) to ensure reversibility is real, not theoretical.
    - **Anti-Lock-in APIs:** For cloud services, mandate the implementation of standard, vendor-neutral APIs (like S3 for storage, or OIDC for identity) rather than proprietary APIs that force code rewrites during migration.
- *Sources: CNLL Position on Interoperability; Cloud-Edge Roadmap (Pillar 1).*

5. Support "Permissionless Innovation" in AI

Context: The AI "Black Box." If the future of software is AI, and AI models are closed, European sovereignty is dead. Relying on "Open AI" (the company) is the opposite of Open Source.

- **The Proposition:** Ensure that EU industrial policy actively discriminates in favor of **Open Science AI** to prevent monopolization.
- **Detailed Action:**
    - **The "Three Opens":** EU funding for AI must require: **Open Weights** (the model), **Open Data** (the training set description/access), and **Open Code** (the training/inference scripts).
    - **Sovereign Training Infrastructure:** Guarantee affordable access to EuroHPC supercomputers for European open source AI developers, on the condition that their output remains open (preventing the privatization of public compute resources).
    - **Legal Clarity:** Explicitly clarify in the AI Act implementation that open source developers and non-commercial researchers are in a "Safe Harbor" regarding liability, to prevent a chilling effect on EU AI innovation.
- *Sources: CNLL/APELL positions on AI Act; Cloud-Edge Roadmap.*

6. Facilitate a "Technical Assistance Facility"

Context: The "Capability Gap." A small municipality or hospital wants to use sovereign open source, but lacks the engineering talent to integrate disparate components. They default to Microsoft/Google because it's an "integrated suite," even if illegal (Schrems II).

- **The Proposition:** Create a mechanism (potentially via the **DC-EDIC**) to act as a **Technical Assistance Facility** for the public sector.
- **Detailed Action:**
    - **Migration Coaching:** Fund experts to help public administrations map their current dependencies and design migration paths to open source.
    - **The "White List" (Solutions Directory):** Maintain a dynamic catalog of **verified, industrial-grade European Open Source solutions** that meet the "Sovereignty Risk Assessment" (Point 1). This de-risks the choice for public CIOs.

  - **Pre-Packaged Distributions:** Fund the packaging of the "Reference Architectures" (Point 2) into easy-to-deploy distributions that competing European hosters can offer as a managed service.
- *Sources: EuroStack position on DC-EDIC; Cloud-Edge Roadmap (Pillar 3).*

Pillar 2: Public Procurement as a Market Shaper

Strategic Objective: Leverage the massive purchasing power of the European public sector (approx. €2 trillion/year, or 14% of GDP) to de-risk the market for European SMEs, break vendor lock-in, and enforce digital sovereignty through the "power of the purse."

7. Enact "Open Source First" Legislation (The "Comply or Explain" Principle)

Context: Voluntary guidelines (like the EIF) have failed to shift market behavior significantly. Public buyers exhibit "defensive buying" inertia, defaulting to large proprietary incumbents due to perceived safety, despite the long-term risks of lock-in and data leakage.

- **The Proposition:** Elevate "Open Source First" from a recommendation to a **binding legal principle** in public procurement directives.
- **Detailed Mechanism:**
  - **Reversal of the Burden of Proof:** Public buyers should default to Open Source solutions. If a proprietary solution is chosen, the buyer must publish a **"Comply or Explain"** justification.
  - **Public Justification Requirements:** The explanation must explicitly address why an existing open source alternative was rejected. It must quantify the **Exit Costs** (cost to migrate away in the future) and verify the **Data Sovereignty** status of the chosen proprietary tool.
  - **Transparency:** These justifications should be publicly searchable to allow scrutiny by civil society and the OSS ecosystem, creating accountability for lazy procurement.
- *Sources: APELL (Measure 3); Cloud-Edge Roadmap (Pillar 3); CNLL Position.*

8. Mandate "European Preference" in Service Procurement

Context: While software code is global, the **legal jurisdiction** of the service provider is local. Buying maintenance, support, or cloud services for open source software from a non-EU company negates the sovereignty benefits, as the service remains subject to extraterritorial laws (e.g., FISA 702).

- **The Proposition:** While the software code can be international, the **contracting entity** for integration, hosting, maintenance, etc., should ideally be European.
- **Detailed Mechanism:**
  - **Jurisdictional Tenders:** Tenders for critical systems should require the prime contractor to be **headquartered** in the EU/EEA and not subject to extraterritorial control orders from foreign governments.
  - **Economic Value Retention:** This ensures that tax revenues and high-skilled jobs (support engineers, R&D) remain in Europe. Even if the core software is global (e.g., Linux), the *value-added layer* (security hardening, integration, managed services) is provided by European industry.
  - **Legal Recourse:** A European public administration must have legal recourse under EU law against its critical IT suppliers, which is difficult when contracting with EU subsidiaries of foreign entities shielded by parent company jurisdictions.
- *Sources: Cloud-Edge Roadmap (Pillar 3); CNLL Doctrine on Strategic Autonomy.*

9. Implement Binding "Sovereignty Criteria" (Pass/Fail)

Context: Current tenders often focus purely on feature lists ("functional requirements") which are easily gamed by incumbents, ignoring the strategic risks of the supplier's origin.

- **The Proposition:** Introduce mandatory **non-functional criteria** related to digital sovereignty in all public tenders for critical digital infrastructure.

- **Detailed Mechanism:**
  - **Legal Immunity:** For critical data, the vendor must guarantee immunity from non-EU extraterritorial data access requests. This acts as a *de facto* filter against US hyperscalers for sensitive sovereign clouds.
  - **Data Residency & Control:** Mandatory location of data *and* metadata within the EU, with operations performed by EU-cleared personnel (sovereign operations).
  - **Full Code Auditability:** The vendor must be able to provide the full source code for security auditing. This effectively disqualifies proprietary "black boxes" where the client cannot verify security claims.
- *Sources: EuroStack (Criteria definition); APELL; CNLL.*

10. Break the "Intermediary Value Trap" (Allotment Strategy)

Context: This is the most critical economic failure identified by the CNLL. Public administrations sign massive framework contracts with large Systems Integrators (ESNs - *Entreprises de Service du Numérique*). These integrators deploy Open Source software but keep the margin, paying zero or negligible amounts to the actual Software Vendors (*Éditeurs*) who create and maintain the code. This starves the producers of the technology.

- **The Proposition:** Issue specific guidance on **Allotment (*Allotissement*)** to ensure value flows to the creators.
- **Detailed Mechanism:**
  - **Separation of Concerns:** Public tenders involving OSS should be split into at least two distinct lots:
    1. **Lot 1: Software Subscription/Support:** Contracted directly with the Software Publisher (or their authorized distributor). This covers "Vendor Support," security patches, roadmap influence, and R&D funding.
    2. **Lot 2: Integration & Managed Services:** Contracted with Systems Integrators for deployment, customization, and training.
  - **Fair Share:** This ensures that the SME writing the code receives recurring revenue, allowing them to invest in security and innovation, rather than the Integrator capturing all the value while contributing nothing to the upstream maintenance.
- *Sources: CNLL (15+ years of market observation); Cloud-Edge Roadmap (Growth & Investment).*

11. Mandate "Public Money, Public Code"

Context: The public sector often pays for custom software development (e.g., a new portal for a ministry) but allows the contractor to keep the IP or simply forgets to publish the code. This is a waste of public funds and prevents reuse by other member states.

- **The Proposition:** Software developed specifically for the public sector with public funds must be **Open Source by Default**.
- **Detailed Mechanism:**
  - **Default Licensing:** Contracts for custom development must mandate delivery under an OSI-approved license (e.g., EUPL).
  - **Repository Requirement:** The delivered code must be published in a public repository (e.g., code.europa.eu or national equivalent) before final payment is released.
  - **Exemptions:** Exceptions for security-sensitive logic (e.g., fraud detection algorithms) or third-party IP must be justified and minimized (e.g., segregating sensitive configuration from the open codebase). Exemptions should concern only the sensitive parts, and not be used as an excuse to not publish anything at all.
- *Sources: FSFE; APELL; Cloud-Edge Roadmap.*

12. Support a "White List" / Solutions Directory (Industrial Grade)

Context: Public buyers are risk-averse. They fear "abandonware" or hobbyist projects. They need a trusted signal that a specific European OSS solution is enterprise-ready.

- **The Proposition:** The Commission (potentially via the DC-EDIC, or another structure dedicated to the promotion of Open Source) should support the maintenance of a **Catalog of Industrial-Grade European Open Source Solutions**.
- **Detailed Mechanism:**
  - **Vetting Criteria:** Inclusion in the catalog is not automatic. Solutions must pass the "Sovereignty Risk Assessment" (Pillar 1) and demonstrate **Industrial Maturity** (active maintenance, existence of a legal entity for support, GDPR compliance, SBOM availability).
  - **Not a Repository, a Buyer's Guide:** This is not GitHub. It is a procurement aid that lists: "Here is the software, here is the European company that provides enterprise support, here are the references in other public administrations."
- *Sources: Cloud-Edge Roadmap (Pillar 3); EuroStack Directory Project.*

13. Mandate TCO Calculation including Exit Costs

Context: Proprietary vendors often win tenders with low initial prices (discounted licenses) but trap administrations with massive price hikes later. Because migration is technically difficult (lock-in), administrations cannot leave.

- **The Proposition:** Procurement rules must require a **Total Cost of Ownership (TCO)** calculation that includes the **Exit Strategy**.
- **Detailed Mechanism:**
  - **Reversibility Cost:** Tenders must evaluate the cost of extracting data and migrating to a rival solution at the end of the contract.
  - **The OSS Advantage:** Since OSS uses open standards and has no license fees, its "Exit Cost" and long-term TCO are significantly lower. Making this calculation mandatory exposes the hidden costs of proprietary lock-in.
- Sources: *CNLL; Cloud-Edge Roadmap.**

14. Leverage Pre-Commercial Procurement (PCP)

Context: Sometimes, the market does not yet offer a sovereign solution for a specific need (e.g., a specific AI tool for healthcare).

- **The Proposition:** Use **Pre-Commercial Procurement (PCP)** instruments to co-fund the development of missing open source building blocks.
- **Detailed Mechanism:**
  - **Market Creation:** The public sector acts as the "first customer," defining the need and funding the R&D phase for a consortium of European SMEs to build the solution.
  - **Open Output:** The resulting IP is released as Open Source, creating a new "common" that the private sector can then commercialize and support.
- Sources: *Cloud-Edge Roadmap (Pillar 3).*

Pillar 3: Investment & Financing the Digital Public Good

Strategic Objective: Solve the "Dual Tragedy of the Commons" (under-provision of maintenance resources vs. over-exploitation by commercial free-riders) and the "Innovation Trap" (funding only new features, never maintenance) through structured, long-term financing.

15. Operationalize the EU Sovereign Tech Fund (EU-STF)

Context: The current EU funding landscape (Horizon Europe, Digital Europe) is designed for *Innovation* (creating new technologies/features) and *Research*. It is structurally incapable of funding **Maintenance** (security hardening, refactoring, bug fixing, documentation) of existing, mature technologies. This leaves critical infrastructure (Open Digital Base Technologies - ODBTs) vulnerable (e.g., the Log4j crisis).

- **The Proposition:** Establish a permanent financial instrument, the **EU Sovereign Tech Fund**, modeled on the successful German *Sovereign Tech Fund*.
- **Detailed Mechanism:**
  - **Scope:** Strictly focused on "Upstream" technology—libraries, protocols, build chains, and kernels that underpin the European digital economy. It excludes commercial "Downstream" products (apps).
  - **Modality:** Unlike research grants (which are slow and bureaucratic), the EU-STF must use **agile procurement** to contract directly with maintainers (individuals, non-profits, or SMEs) for specific roadmaps.
  - **Budget:** A recommended minimum of **€350M** over 7 years to ensure critical mass.
  - **Implementation:** This could be implemented via a dedicated agency or by leveraging the **DC-EDIC** as a vehicle to pool Member State contributions alongside Commission funding.
- *Sources: OFE Feasibility Study (Comprehensive design); Cloud-Edge Roadmap (Pillar 4); German STF experience.*

16. Incentivize Private Co-Investment (Tax Credits & Matching)

Context: Large non-EU corporations generate billions in revenue using Open Source components but often contribute little back to the European maintenance ecosystem ("Free-Riding"). Voluntary contribution models have proven insufficient.

- **The Proposition:** Use fiscal policy to incentivize private companies to invest in the open source builiding blocks they rely on.
- **Detailed Mechanism:**
  - **Tax Credits for Contribution:** Introduce a specific tax credit (similar to the R&D Tax Credit in France) for developer time spent contributing to recognized Open Source projects or foundations.
  - **Matching Funds:** Create a mechanism where the EU matches private donations to qualified European Open Source Foundations (e.g., Eclipse, OW2, Apache Europe). If a European SME donates €50k to secure a library, the EU adds €50k, doubling the impact.
  - **Conditionality:** These incentives must be tied to **public code contributions** or direct financial support to the project governance, not internal R&D that remains proprietary.
- *Sources: OFE Feasibility Study; Cloud-Edge Roadmap (Growth & Investment).*

17. Establish a European Open Source Investment Platform (EOSIP)

Context: European investors (VCs) often struggle to understand Open Source business models. They look for "IP ownership" and "Licensing moats," whereas Open Source business models rely on service, support, and "Open Core" strategies. This leads to a funding gap for OSS startups in the scale-up phase.

- **The Proposition:** Create a specialized investment platform or "Fund of Funds" to de-risk investment in OSS SMEs.
- **Detailed Mechanism:**
  - **Education for Investors:** Provide training to European investment banks and VCs on how to value Open Source companies (valuing community traction and adoption over IP locking).
  - **De-Risking:** Use **InvestEU** guarantees to back private funds that specialize in Open Source technologies (Deep Tech).
  - **Sovereignty Clause:** Investment agreements should include clauses preventing the transfer of critical IP or governance control to non-EU entities during future exit/acquisition events (preventing the "buy and close" strategy of US competitors).

- *Sources: Cloud-Edge Roadmap (Pillar 4).*

18. Support and Institutionalize "Blue Hats" Communities

Context: The "Blue Hats" concept (civil servants contributing code back to the digital public goods) is currently a collection of informal initiatives or best practices (e.g., in France's DINUM). It lacks institutional weight, budget, and legal clarity.

- **The Proposition:** Transform "Blue Hats" from a community of practice into a **funded institutional program**.
- **Detailed Mechanism:**
  - **Legal Framework:** Provide clear legal guidelines (or a directive) allowing public sector employees to contribute code and time to external Open Source projects during working hours without intellectual property friction.
  - **Time Budgeting:** Encourage public administrations to allocate a specific percentage of IT staff time (e.g., 10%) to upstream contribution, recognizing this as "preventative maintenance" for their own infrastructure.
  - **Recognition:** Create EU-level awards and recognition for public administrations that are top contributors, fostering a culture of prestige around code contribution.
- *Sources: CNLL; DINUM (France); Cloud-Edge Roadmap (Pillar 2).*

19. Redirect and Earmark Horizon / Digital Europe Funds

Context: Billions are spent on research (Horizon Europe), but the software outputs often become "abandonware" once the grant ends because there is no funding for the transition from "Research Prototype" to "Industrial Product," nor for the maintenance of the underlying grassroots ecosystem. Large consortia monopolize funding, while the SMEs and individual maintainers building the actual Digital Commons are excluded by administrative complexity.

- **The Proposition:** Rebalance existing funds to support the **lifecycle** of software (maintenance) and **grassroots innovation** (small players).
- **Detailed Mechanism:**
  - **Institutionalize "Cascade Funding" (FSTP):** The Commission must make **Financial Support to Third Parties** (Cascade Funding) a standard instrument across Digital Europe and Horizon Europe. As proven by the **Next Generation Internet (NGI)** initiative—which successfully funded over 1,000 projects—this is the only mechanism agile enough to reach the deep-tech SMEs and maintainers who build the **Open Internet Stack**. Abandoning this model would sever the lifeline of the European grassroots ecosystem.
  - **Earmarked Maintenance Calls:** Launch calls dedicated *exclusively* to the maturation, documentation, and security hardening of existing European OSS prototypes. Banning the development of "new features" in these calls forces a focus on stability and industrial readiness.
  - **The "Sustainability Check":** Require all software-heavy Horizon Europe projects to include a funded plan for transfer to an Open Source Foundation or continued community maintenance after the project ends.
  - **Open Science Default:** Mandate that software produced by EU-funded research must be Open Source (Open Science), preventing the privatization of public research results.
- *Sources: Cloud-Edge Roadmap (Pillar 4); CNLL Position on NGI (2024).*

Pillar 4: Skills, Education & Workforce

Strategic Objective: Build a sovereign talent pipeline to reduce reliance on non-EU expertise and correct the "vendor lock-in of the mind" that occurs when students are trained solely on proprietary platforms.

20. Integrate OSS into STEM Curricula (Primary to University)

Context: Currently, many European educational institutions act as sales channels for non-EU hyperscalers (e.g., "Google Classroom", "Microsoft for Education"), training students to be consumers of specific proprietary products rather than digitally literate citizens. This creates a long-term cultural lock-in.

- **The Proposition:** Mandate the integration of Open Source principles, development practices, and legal frameworks into national computer science and civic education curricula.
- **Detailed Action:**
  - **Digital Civics:** Teach the concepts of open standards, data privacy, and digital sovereignty as part of general digital literacy, using OSS tools to demonstrate transparency.
  - **Technical Curricula:** Computer Science degrees must include mandatory modules on **OSS Licensing** (IP law), **Community Governance**, and **Distributed Development** (Git flows, peer review).
  - **Infrastructure:** Encourage schools and universities to use open source software for their own operations (LMS, cloud), serving as a real-world example to students ("Practice what you teach").
- *Sources: Cloud-Edge Roadmap (Pillar 2); CNLL Advocacy; APELL.*

21. Create EU-Recognized Certifications (Countering Proprietary Standards)

Context: HR departments and public tenders often require certifications like "AWS Certified" or "Microsoft Certified Professional." There is a lack of recognized credentials for European/Sovereign technologies, making it hard for European engineers to prove their value and for companies to hire them.

- **The Proposition:** Develop and promote a standard framework of **European Digital Sovereignty Certifications**.
- **Detailed Action:**
  - **Standardization:** Collaborate with industry bodies to create certifications for key roles: "Certified European Cloud Architect," "Sovereign Identity Specialist," or "Open Source Compliance Officer."
  - **Recognition:** Ensure these certifications are recognized in public procurement tenders as valid proof of technical capacity, equivalent to or preferred over vendor-specific proprietary certifications.
  - **Focus on ODBTs:** Certifications should focus on the underlying open technologies and standards (e.g., POSIX/Single Unix Specification/Linux Standard Base/…, Matrix, etc.) rather than a specific vendor's implementation, promoting workforce mobility and resilience.
- *Sources: Cloud-Edge Roadmap (Pillar 2 - Skills Development).*

22. Launch "Open Source Business" Vocational Training

Context: Europe produces brilliant code but often fails to build sustainable businesses around it. Many creators give up or sell to US companies because they lack expertise in **Open Source Business Models** (e.g., Open Core, SaaS, Support subscriptions) and IP strategy.

- **The Proposition:** Create targeted vocational training programs for entrepreneurs, SME managers, and incubator cohorts.
- **Detailed Action:**
  - **Curriculum:** Focus on monetization strategies that respect open source values while ensuring revenue (avoiding the "free work" trap). Teach defensive IP strategy and community management.
  - **Target Audience:** Deep-tech startups, university spin-offs, and SMEs looking to pivot from a "custom development" service model to a "software publisher" product model.
  - **Public Purchasers Training:** *Crucially*, extend this training to public procurement officers so they understand the difference between purchasing a license and purchasing a subscription/maintenance contract for OSS.
- *Sources: CNLL (PME support); Cloud-Edge Roadmap (Pillar 2).*

23. Establish "Centres of Excellence" in Universities

Context: The maintenance of critical "deep tech" layers (kernels, compilers, cryptography) requires highly specialized skills that are becoming rare. There is a risk of a "brain drain" of these specialists to non-EU tech giants.

- **The Proposition:** Fund university-based **Centres of Excellence for Open Digital Infrastructure**.
- **Detailed Action:**
  - **Research & Maintenance:** These centres should not just do abstract research but actively participate in the maintenance of critical global projects (e.g., the Linux Kernel, GCC, cryptographic libraries), ensuring Europe retains "maintainer seats" at the global table.
  - **Dual Track:** Offer tracks for both academic research and applied engineering, allowing students to get academic credit for contributing to major open source projects.
- *Sources: Cloud-Edge Roadmap (Pillar 2); EuroStack.*

24. Promote Diversity & Inclusion in the Contributor Community

Context: The open source contributor base is historically homogenous. This limits innovation and excludes large segments of the European population from the digital economy.

- **The Proposition:** Create specific grant programs and mentorship initiatives to support under-represented groups.
- **Detailed Action:**
  - **Fellowships:** Provide stipends for women and under-represented minorities to work on open source projects, mirroring successful programs like "Outreachy" but with EU funding and a focus on European strategic projects.
  - **Safe Spaces:** Enforce Codes of Conduct in EU-funded projects to ensure welcoming environments for diverse contributors.
- *Sources: APELL; General ecosystem best practices.*

Pillar 5: Governance & Regulatory Coherence

Strategic Objective: Move from a fragmented landscape to a unified European voice. Ensure that the legal environment provides certainty and protection for open collaboration, preventing "regulatory chill."

25. Implement a Mandatory "OSS Check" (Impact Assessment)

Context: Recent legislative initiatives (e.g., the Cyber Resilience Act, the Product Liability Directive) created near-existential crises for the open source ecosystem because they were initially drafted with proprietary, vertical business models in mind. They failed to account for the decentralized, often non-commercial nature of open source production.

- **The Proposition:** Introduce a systematic, mandatory **Open Source Impact Assessment** for all new digital legislation *before* it enters the legislative process.
- **Detailed Mechanism:**
  - **Structural Evaluation:** Every Digital DG proposal must evaluate its impact on: non-profit foundations, individual developers, and SME-led open source projects.
  - **The "Sovereignty Test":** Legislation must be checked to ensure it does not inadvertently advantage non-EU hyperscalers (who have large compliance departments) over European open source SMEs (who do not).
  - **Consultation Protocol:** Mandatory consultation with representative bodies of the OSS industry (like APELL/CNLL) during the drafting phase, not just the public consultation phase.
- *Sources: APELL (Measure 4); CNLL Response to CRA.*

26. Appoint an "Open Source Envoy"

Context: Open Source touches competition policy (DG COMP), industrial strategy (DG GROW), research (DG RTD), and internal IT (DG DIGIT). Currently, responsibility is fragmented, leading to policy incoherence (e.g., funding open source in Horizon Europe while threatening it with liability in the CRA).

- **The Proposition:** Designate a **European Open Source Envoy**, a high-level official with a political mandate to champion the sector.
- **Detailed Mechanism:**
  - **Cross-Directorate Mandate:** The Envoy coordinates between DGs to ensure the "1-2-3 Principle" (Open Source First, European Preference, Risk Assessment) is applied consistently.
  - **Ambassador Role:** The Envoy represents the EU's open source strategy to Member States, urging them to align national policies, and serves as the primary interlocutor for the ecosystem.
  - **Sovereignty Guardian:** This role specifically oversees the "Sovereignty Risk Assessments" to ensure they are not diluted by foreign lobbying.
- *Sources: APELL (Measure 3); Cloud-Edge Roadmap (Governance).*

27. Formalize and Fund the Network of OSPOs

Context: The European Commission's OSPO is a success, as are national initiatives like Germany's ZenDiS or France's Mission Logiciels Libres. However, they operate largely as a loose coalition of the willing.

- **The Proposition:** Institutionalize the **European Network of OSPOs** as a funded, operational body.
- **Detailed Mechanism:**
  - **Connecting the Layers:** Create a formal structure linking the EC OSPO, Member State OSPOs, and Regional/City OSPOs.
  - **Mutualization:** Use this network to share code (Inner Source becoming Open Source), procurement templates, and legal analysis. If one country audits a piece of software, the result is shared instantly across the network.
  - **Capacity Building:** Provide funding to help smaller Member States establish their own national OSPOs.
- *Sources: CNLL Position Paper on OSPOs; OFE; Cloud-Edge Roadmap.*

28. Create Legal "Safe Harbors" for Maintainers

Context: The fear of liability is a massive barrier. If an individual or an SME publishes code for free, they should not be liable for millions of euros in damages if a bank uses it and gets hacked. Without clear boundaries, European developers will stop publishing code or move to jurisdictions with better protections.

- **The Proposition:** Explicitly codify the **"Upstream Exemption"** in EU law.
- **Detailed Mechanism:**
  - **Commercial vs. Non-Commercial:** Clear legal definitions distinguishing between "placing a product on the market" (commercial activity subject to liability) and "publishing code" (free speech/scientific contribution exempt from liability).
  - **Steward Protection:** Specific legal protections for non-profit Open Source Foundations (Stewards) that host infrastructure but do not control the commercial use of the software.
- *Sources: APELL; OFE Feasibility Study; CRA*

D. What technology areas should be prioritised and why?

Based on the "risk-based" doctrine and the industrial analysis provided by the **Cloud-Edge Alliance Roadmap** and **EuroStack**, the prioritization of technology areas should not be based on "trends," but on **Strategic Dependency** and **Industrial Potential**.

The Commission must prioritize areas where **Vendor Lock-in is currently highest** (posing an economic threat) and where **Extraterritorial Risk is most acute** (posing a sovereignty threat).

We propose prioritizing four strategic clusters:

1. The Cloud-Edge-IoT Continuum (The Industrial Backbone)

Context: As detailed in the *Cloud-Edge Alliance Roadmap*, this is the battlefield for Industry 4.0. Currently, the market is dominated by non-EU hyperscalers, creating a risk that European industrial data (factory data, energy grids, mobility) becomes captured in proprietary silos subject to foreign jurisdiction.

- **Priority Technologies:**
  - **Orchestration & Containerization:** cloud orchestration and management tools that allow workloads to move freely between clouds (reversibility).
  - **Edge Computing Operating Systems:** Lightweight, secure open OS for industrial controllers and IoT gateways, preventing a "Android-ization" of European industry by non-EU platforms.
  - **Federated Data Infrastructure:** Connectors and dataspace components (based on DSBA standards) to enable secure data sharing without centralization.
- **Why Prioritize?**
  - **Sovereignty:** To ensure European industrial data remains under EU jurisdiction.
  - **Resilience:** Edge computing requires autonomy; a factory must keep running even if the connection to a US cloud is severed.

2. The Digital Workplace & Collaboration (The Public Sector Lock-in)

Context: This is the primary source of value leakage in the public sector. As noted by the **CNLL**, public administrations are massively dependent on Microsoft 365 and Google Workspace. This creates a "default" lock-in that dictates identity management, document formats, and communication channels, making it nearly impossible to switch.

- **Priority Technologies:**
  - **Sovereign Collaboration Suites:** Platforms combining file storage, document editing, chat, and video conferencing (e.g., XWiki, Matrix-based solutions, Jitsi/BigBlueButton/Galene, etc.).
  - **The "Sovereign PC" (EU Linux / EU OS):** A secure, Linux-based desktop operating system for public servants (as proposed in the *EU OS* project presentation) to break the hardware-software obsolescence cycle mandated by proprietary vendors (e.g., Windows 11 requirements).
  - **Interoperable Office Formats:** Strict enforcement of ODF (Open Document Format) over proprietary OOXML to ensure long-term archival sovereignty.
- **Why Prioritize?**
  - **Economic Efficiency:** Stopping the massive outflow of license fees for "commodity" software.
  - **Legal Immunity:** Ensuring citizen data processed by civil servants (emails, documents) is never exposed to extraterritorial scanning.

3. Cybersecurity, Identity & Supply Chain (The Trust Layer)

Context: Security cannot be a "black box." The implementation of the **Cyber Resilience Act (CRA)** and **eIDAS 2.0** requires technologies that are fully auditable. Relying on proprietary security tools from non-EU vendors to protect European infrastructure is a strategic paradox.

- **Priority Technologies:**
  - **Digital Identity Wallets (EUDI):** The reference implementations for the European Digital Identity Wallet must be fully open source to ensure citizen trust and prevent capture by private platforms (Apple/Google).

  - **Supply Chain Security Tools:** Automated tooling for generating Software Bills of Materials (SBOMs), vulnerability scanning, and reproducible builds.
  - **Post-Quantum Cryptography:** Open implementations of PQC algorithms to prepare European infrastructure for the quantum threat without relying on NSA-approved black boxes.
- **Why Prioritize?**
  - **Trust:** Only open source allows for the collective verification required for critical identity and security infrastructure.
  - **Compliance:** To enable European SMEs to comply with the CRA without prohibitive costs.

4. Open Source AI & Data Infrastructure (The Future Frontier)

Context: There is a high risk that Artificial Intelligence becomes a “duopoly” controlled by US and Chinese tech giants. If the foundational models are proprietary, European innovation will be limited to “fine-tuning” rented models, creating a permanent dependency rent.

- **Priority Technologies:**
  - **Open Weights Models:** Foundational models where the weights are public and the license permits commercial use without restrictions.
  - **Open Training Datasets:** Curated, legally cleared, multilingual European datasets (High-Performance Language Technologies) to train models that respect European cultures and languages.
  - **AI Toolchains:** Open source libraries for training and inference (e.g., PyTorch, scikit-learn) to ensure Europe retains the *capability* to build AI, not just use it.
- **Why Prioritize?**
  - **Permissionless Innovation:** Preventing a scenario where European startups must ask permission (and pay API fees) to a non-EU gatekeeper to innovate.
  - **Cultural Sovereignty:** Ensuring AI models reflect European languages and values, not just English-centric data.

Summary of Priorities based on the “1-2-3 Doctrine”

Priority Area	Strategic Goal	Key “Sovereignty Criterion”
Cloud & Edge	**Industrial Autonomy**	Data Residency & Reversibility
Digital Workplace	**Public Sector Independence**	Legal Immunity & Zero Exit Costs
Cybersecurity/ID	**Trust & Compliance**	Full Code Auditability
Artificial Intelligence	**Future Competitiveness**	Open Weights & Open Data

E. In what sectors could an increased use of open source lead to increased competitiveness and cyber resilience?

Based on the sectoral analysis provided in the **Cloud-Edge Alliance Roadmap** and the strategic priorities identified by the **CNLL** and **APELL**, we identify five strategic sectors where the shift to Open Source is not merely an IT upgrade, but a prerequisite for **survival, sovereignty, and competitiveness**.

In these sectors, the “Risk-Based Approach” (Pillar 1) is paramount: reliance on “black box” proprietary software creates unacceptable systemic risks.

1. Public Administration: The Anchor of Sovereignty

Context: Public administrations are the largest collectors of citizen data. Currently, the sector suffers from high fragmentation and massive value leakage through licensing fees to non-EU vendors (e.g., the Microsoft Office monopoly).

- **Cyber Resilience Gains:**
  - **Continuity of Public Service:** Open Source ensures that public services cannot be "switched off" by a foreign entity via sanctions or license revocation.
  - **Auditability:** As highlighted by the **EU OS** project, government workstations and servers are critical targets. Open source allows for collective security auditing of the code running the state, replacing blind trust with verification.
- **Competitiveness Gains:**
  - **Local Economic Multiplier:** Shifting budget from "Global Licenses" to "Local Services" (integration, maintenance) reinjects tax money into the European SME ecosystem (addressing the *Intermediary Value Trap*).
  - **Interoperability:** Mandating open standards prevents data silos between ministries, reducing administrative friction and cost.

2. Industry 4.0 & Manufacturing: Protecting the Value Chain

Context: Europe is a global leader in industrial machinery. As factories become software-defined, there is a risk of "value capture" where non-EU hyperscalers provide the "smart" layer (Cloud/AI), reducing European manufacturers to mere hardware assemblers ("commoditization").

- **Cyber Resilience Gains:**
  - **Edge Autonomy:** Factories must continue to operate even if the connection to the cloud is severed. Open source Edge Computing (as detailed in the *Cloud-Edge Roadmap*) allows for local, autonomous processing of industrial data.
  - **Security through Obscurity is Dead:** Industrial control systems (ICS) are prime targets for cyberwarfare. Open source stacks allow manufacturers to patch vulnerabilities instantly without waiting for a legacy vendor's timeline.
- **Competitiveness Gains:**
  - **Avoiding the "Android-ization" of Industry:** By controlling the open source platforms (e.g., Eclipse-based industrial IoT stacks), European manufacturers retain control over the data interface, preventing non-EU platforms from extracting the industrial data value.

3. Healthcare: Data Privacy and Research Velocity

Context: Health data is the most sensitive category under GDPR. The sector is currently plagued by proprietary vendor lock-in that makes sharing patient data between hospitals technically and legally difficult.

- **Cyber Resilience Gains:**
  - **Data Sovereignty:** Open source Electronic Health Records (EHR) and infrastructure allow data to be hosted strictly within sovereign bounds (SecNumCloud, etc.), ensuring immunity from extraterritorial data access (FISA).
  - **Long-Term Access:** Medical records must remain readable for decades. Open standards guarantee that data is not lost if a proprietary vendor goes bankrupt or sunsets a product.
- **Competitiveness Gains:**
  - **Accelerated Research:** Open source AI models and data frameworks allow research institutions to collaborate on drug discovery and diagnostics without navigating complex IP licensing webs for every tool used.

4. Energy & Utilities: Securing the Green Transition

Context: The transition to Smart Grids and renewables requires connecting millions of devices (solar inverters, EV chargers, smart meters) from different vendors. Proprietary silos inhibit this necessary orchestration.

- **Cyber Resilience Gains:**
  - **Supply Chain Transparency:** Critical infrastructure requires a complete Software Bill of Materials (SBOM). Only open source allows utilities to fully map their software dependencies and assess risks (e.g., identifying a compromised library in a smart meter fleet).
- **Competitiveness Gains:**
  - **Standardization of the Edge:** An open source "energy operating system" (like the projects under the *Linux Foundation Energy*) allows European utilities to standardize device communication, lowering the barrier to entry for European hardware startups and integrators.

5. Education & Research: The Talent Pipeline

Context: As noted many times over the years by the **CNLL**, education is currently a primary vector for vendor lock-in. Students trained exclusively on proprietary non-EU platforms enter the workforce with a bias that perpetuates dependency.

- **Cyber Resilience Gains:**
  - **Privacy by Design:** Schools handle data of minors. Open source platforms (e.g., Moodle, BigBlueButton) allow this data to be kept within school districts or national clouds, protecting children from data profiling by advertising giants.
- **Competitiveness Gains:**
  - **Deep Tech Skills:** Students learning on Open Source systems can inspect the code and understand *how* it works. This produces engineers and creators, whereas proprietary tools produce mere *users*. This is the foundation of the future workforce required for Pillar 4 (Skills).

General Conclusion

The Conseil National du Logiciel Libre (CNLL), representing the French Open Source industry, urges the European Commission to recognize that the era of "laissez-faire" in digital policy is over. The shift to Open Source is no longer a matter of technical detail or a "nice-to-have" option; it is a **structural macro-economic imperative**.

It represents the fundamental choice between a Europe that **rents** its digital future from foreign entities—remaining vulnerable to extraterritorial laws, price hikes, and supply chain shocks—and a Europe that **owns, secures, and maintains** its own critical infrastructure.

The path to sovereignty requires moving from observation to industrial action. By implementing the measures outlined in this consultation response, the Commission can unlock the immense potential of the European ecosystem.

The time for fear and lamentation is over. The tools, the strategies, and the will exist. What we need now is action. The Commission has the power to reshape Europe's digital landscape—to move from dependency to sovereignty, from fragmentation to cohesion, and from observation to leadership. The European Open Source industry is mature, aligned with European values, and ready to deliver. We call on the Commission to provide the industrial policy framework that matches this ambition. The future of our digital sovereignty is in our hands—let's build it.

References & Supporting Documentation

I. Industry Position Papers & Strategic Doctrine

- **APELL (Association Professionnelle Européenne du Logiciel Libre)**
  - *Feedback on the Communication "Towards European Open Digital Ecosystems"* (30 January 2026).
  - *Submission to the Evaluation of Public Procurement Directives* (February 2025).
  - *Statement on the Cyber Resilience Act (CRA)* (September 2023).
- **CNLL (Conseil National du Logiciel Libre)**
  - *Position Paper: A Proposal for a Coordinated European Model of Open Source Programme Offices (OSPOs)* (July 2025).
  - *Propositions pour une politique industrielle du logiciel libre* (2024).
  - *« Le logiciel libre et l'ouverture des données sont deux enjeux majeurs du numérique moderne qui méritent une stratégie publique »* (Le Monde, 2021)
- **EuroStack Initiative**
  - *White Paper: Deploying the EuroStack – What's Needed Now* (2025).
  - *A Proposed Framework for a "Buy European" Regulation of Strategic Digital Procurement* (2025)
  - *OPINION. « Souveraineté numérique : l'Europe doit proposer une approche incisive et pragmatique »* (La Tribune, 2025)
- **Euclidia and other collectives**
  - *Tribune: "La construction de notre indépendance numérique est une question de volonté politique"* (Smets, Garnier, Bretones, Hug, Przyluski - Acteurs Public, 2022).
  - Some Thoughts on Interoperability (Stefane Fermigier / EuroStack Directory Project, 2024)

II. Feasibility Studies & Roadmaps

- **European Alliance for Industrial Data, Edge and Cloud**
  - *Thematic Roadmap: The Open Source Way to EU Digital Sovereignty & Competitiveness* (Alliance for Industrial Data, Cloud & Edge, prepared by the Cloud-Edge Working Group, 2025).
- **OpenForum Europe (OFE)**
  - *Funding Europe's Open Digital Infrastructure: A Study on the Economic, Legal, and Political Feasibility of an EU Sovereign Tech Fund (EU-STF)* (Gates, Tridgell, et al., 2025).
- **European Commission**
  - *Study about the impact of Open Source software and hardware on technological independence, competitiveness and innovation in the EU economy* (Blind et al., 2021).

III. Technical Projects & Initiatives

- **EU OS Project**
  - *EU OS: An Operating System for the Public Sector – Status and Next Steps* (Dr. Robert Riemann, October 2025).
- **Digital Commons EDIC (DC-EDIC)**
  - *Announcements by the founding member states* (2025).
  - EuroStack's position on the DC-EDIC (2025).
- **National Initiatives Referenced**
  - *ZenDiS (Zentrum für Digitale Souveränität)* – Germany.
  - *Socle Interministériel de Logiciels Libres (SILL) / Mission Logiciels Libres* – France.

IV. Regulatory Framework Context

- **EU Legislation**

- *Cyber Resilience Act (CRA)* – Regulation on horizontal cybersecurity requirements for products with digital elements.
- *Interoperable Europe Act* – Regulation laying down measures for a high level of public sector interoperability.
- *AI Act* – Regulation laying down harmonised rules on artificial intelligence.
- *Data Act* – Regulation on harmonised rules on fair access to and use of data.

Submitted by:
Conseil National du Logiciel Libre (CNLL)
Date: February 3rd, 2026