OpenForum Europe

RI. SE

SACHIKO MUTO, CHAIR, OFE & SENIOR RESEARCHER, RISE

A strategic approach to open source in the EU

National Open Source Innovation Summit 2026, Dublin

About me

- Chair and former CEO, OpenForum Europe
- Senior Researcher, RISE Research Institutes of Sweden
- Drupal Association Board Member
- Advisory Board member Linux Foundation Europe and Linux Foundation Research
- Engaging policymakers on open source since 2007 — now witnessing an unprecedented focus on open source as a key enabler of digital sovereignty.

RI.
SE

European Open Digital Ecosystems

In preparation

Call for evidence

Feedback period

06 January 2026 - 03 February 2026

Feedback: Open

About this initiative

Summary

The European Open Digital Ecosystem Strategy will set out:

- a strategic approach to the open source sector in the EU that addresses the importance of open source as a crucial contribution to EU technological sovereignty, security and competitiveness
- a strategic and operational framework to strengthen the use, development and reuse of open digital assets within the Commission, building on the results achieved under the 2020-2023 Commission Open Source Software Strategy.

Political context

President von der Leyen's political guidelines, the mission letter for Executive Vice-President for Tech Sovereignty, Security and Democracy Virkkunen and the 2025 State of the Union speech identified EU technological sovereignty as one of the objectives for this College's term of office.

Against this background, the Commission will set out a strategic approach to the open-source sector in the European Union and present a review of the Commission's 2020-2023 open-source software strategy, which will outline the Commission's plan for its own digital environment. The new strategy will address the economic and political importance of open source, as a crucial contribution to a strategic framework for EU technological sovereignty, competitiveness and cybersecurity. It will also set out actions to strengthen the broader EU open ecosystem of solutions and products in critical sectors, including internet technologies, cloud, artificial intelligence (AI), cybersecurity, open hardware, and industrial applications (e.g. automotive and manufacturing).

Open-source technologies have the potential to enable greater control over digital infrastructure and to reduce the EU's dependencies, ensure greater supply chain transparency and support cybersecurity vulnerability management. Therefore, there is also a case for reviewing what support actions can be put in place to: (i) encourage greater adoption of open source by public and private users, and encourage organisations to contribute to open-source development; (ii) boost the development and competitiveness of the emerging EU open-source sector; and (iii) strengthen the position of start-ups in the innovation ecosystems.

This initiative complements the upcoming Cloud and AI Development Act, for which a dedicated consultation was conducted, and which will be adopted alongside the open-source strategy, as a package.

EUROPEAN COMMISSION

DIRECTORATE-GENERAL FOR DIGITAL SERVICES

Luxembourg

Cloud Sovereignty Framework

Version 1.2.1 – Oct. 2025

RI.
SE

SOV-1: Strategic Sovereignty

- Ensuring that bodies having decisive authority over your services are located within EU jurisdiction.
- Evaluating the assurances against change of control.
- Degree to which the provider relies on financing coming from EU sources.
- Extent of investment, jobs, and value creation within EU.
- Involvement in EU initiatives, Consistency with digital, green, and industrial sovereignty objectives defined at EU level
- Ability to sustain secure operations against requests to cease or suspend the service, or if vendor support is withdrawn or disrupted

RI.
SE

SOV-4: Operation Sovereignty

- Ease of migrating workloads or integrating with alternative EU-controlled solutions without vendor lock-in.
- Capacity for EU operators to manage, maintain, and support the technology without requiring non-EU vendor involvement.
- Existence of an EU-based talent pool with the expertise to operate and sustain the service.
- Assurance that operational support is delivered from within the EU and subject exclusively to EU legal frameworks
- Availability of full technical documentation, source code, and operational know-how enabling long-term autonomy.
- Location and legal control of critical suppliers or subcontractors involved in service delivery.

RI.
SE

SOV-5: Supply Chain Sovereignty

- Geographic source of key physical parts, manufacturing location -countries where hardware is manufactured or assembled
- Jurisdiction and provenance of embedded code controlling hardware, firmware
- Origin of Software: where and by whom software is architected and programmed, location and jurisdiction governing software packaging, distribution, and updates.
- Degree of reliance on non-EU vendors, facilities, or proprietary technologies
- Visibility into the entire supplier and sub-supplier chain, including audit rights.

RI.
SE

Thank you!

sachiko@openforumeurope.org
sachiko.muto@ri.se