Feedback from European Digital Rights (EDRi) on a European Union Strategy

“Towards European open digital ecosystems”

With contributions from EDRi members Access Now and Vrijschrift.org

January 2026

FREE AND OPEN SOURCE SOFTWARE

The main characteristic of open source software is that the source code (i.e. the human-readable instructions written by software developers to create computer programmes) is available for review. There is wide agreement today that making source code available increases the security and trust in software, as it enables third parties to verify what the software does and identify potential flaws or unwanted behaviour.

As an extension of this approach to trustworthy and transparent software development, Free and Open Source Software (FOSS) licences have been developed in order to provide a reliable legal framework for these types of software. 'Free' refers in this context to freedom, not gratis software. The core principle of these FOSS licences is that they commonly not only make source code available in view of increasing trust and security, but also grant everyone the right to use, study, share, and improve the programme for any purpose.

When a licence grants users these four freedoms, the software is considered Free Software. The goals of FOSS are crucial in today's geopolitical reality, as they are a cornerstone for Europe's digital sovereignty ambitions:

1. To prevent undue dependencies on few big tech firms and to reduce vendor lock-in;
2. To enable the open collaboration of public bodies and administrations to address joint software needs;
3. To strengthen this ecosystem as a strategic investment in the EU's long-term technological capacity and independence;
4. To foster innovation within the EU and with democratic partners globally.

In contrast, software that does not provide these freedoms is referred to as 'proprietary' software. Recognised lists of licences are maintained by the Free Software Foundation (FSF), the Open Source Initiative (OSI), and the Debian Project. One definition of FOSS is also contained in Recital 18 of the EU Cyber Resilience Act. In the following paper, the terms Free Software and Open Source Software are used interchangeably with the abbreviation FOSS.

BARRIERS TO OPEN SOURCE ADOPTION

1. What are the strengths and weaknesses of the EU open-source sector? What are the main barriers that hamper (i) adoption and maintenance of high-quality and secure open source; and (ii) sustainable contributions to open-source communities?

The first barrier to a high-quality and secure open source ecosystem for Europe is a lack of investment from its principle benefactors, both private and public.

The global open-source sector, including in the EU, is in a peculiar situation: While the majority of software used today relies one way or another on open source components, applications, or entire operating systems, the software *market* and its profits continue to be dominated and reaped by a small handful of the largest tech firms and their proprietary software products. Some of those tech firms contribute to varying degrees to the development of parts of this massive open source ecosystem, at least where it suits their business needs. Yet these contributions are not nearly sufficient to create and sustain the building blocks needed to meet Europe's digital sovereignty ambitions. Instead, Big Tech is using this open source infrastructure to enable their proprietary products and services which then monopolise the respective markets and funnel all profits into the hands of those companies.

To some extent, the same is true for public administrations that use open source software developed and maintained by a community of volunteers and/or non-profit organisations without contributing to the provision of the stable means needed to do that work. Where public funding is available, it often comes in the form of small pilot projects that do not lead to sustainable long term funding, or it is reserved for the implementation of new functionality that a public administration happens to need at that moment. What is missing is stable financial support for the often unspectacular but crucially important daily maintenance work required by any mid-size to large software product. Moreover, public bodies have developed a tendency to outsource ICT to foreign hyperscalers and Big Tech companies, and in the process lose crucial in-house knowledge. This grants those companies the ability to deprive public administrations from reaping the full benefits of open source ecosystems, and allows them to obtain a dominating presence even in within some open source ecosystems.

The second barrier to a high-quality and secure open source ecosystem for Europe is a lack of commitment from public bodies to use it.

Public procurement accounts for approximately €2 trillion annually or 14% of the EU's GDP. It is one of the largest and most powerful levers in the European economy. A sizeable chunk of this investment goes into IT services, consulting, software development, training and support.

By means of example, Amazon provides its AWS cloud services to over 11,000 government agencies globally, including at federal, national and local levels. Big Tech firms like Amazon, Microsoft, or Alphabet do not publicly disclose how much of their annual revenue stems from government contracts, but it has reasonably been estimated to be in US$ 10-20 billion range, trending upwards every year.

These investments are dearly missing in the open source ecosystem. Every Euro spent by public administrations on proprietary software is lost for the sovereign open source solutions the EU so desperately needs to address the shifting geopolitical threats. Every Euro spent on market-dominant tech firms further entrenches that dominance to the detriment of a competitive, healthy market. And every Euro spent on firms based in countries that have shown to abuse tech dependencies for political intimidation and threats against the EU and its member states is funding Europe's own international weakening.

If the EU and its member states are serious about their digital sovereignty ambitions, they therefore need to drastically scale up public funding for open source technologies that public institutions as well as the rest of the market depend on. Public investments into FOSS is not a subsidy for a product or service but an investment in the digital commons whose societal benefits for Europe multiply every time someone reuses its code.

THE VALUE OF OPEN SOURCE

2. What is the added value of open source for the public and private sectors? Please provide concrete examples, including the factors (such as cost, risk, lock-in, security, innovation, among others) that are most important to assess the added value.

In the past, the dominant model for the public procurement of software was to purchase a specific version of e.g. an operating system or office programme for a fixed amount of money. That programme would then be owned by the public administration in perpetuity. If the purchased software was proprietary (i.e. with closed source code), this could create a certain level of vendor lock-in, but the costs generally remained fixed.

The current dominant delivery model for software is based on 'subscriptions', either of software licences or of Software-as-a-Service (SaaS), where public administrations never own the software but rather rent proprietary solutions for temporary use. With SaaS, the software is not run on users' devices, but on remote servers owned and controlled by the software vendor. This new form of software production and distribution has several major drawbacks for public bodies:

1. The functionality that has been paid for is, in fact, never owned or controlled by the purchasing public administration.

2. Vendors of proprietary SaaS retain complete control over future changes to functionality and availability. Vendors based in adversarial countries or owned by adversaries can stop—or be forced to stop—its provisioning at any time. The same is true for vendors that are overly exposed to adversarial countries through market share.

3. The SaaS-based subscription model means that the integrity and confidentiality of any data processed is vulnerable to adversarial government access (e.g. through the US Cloud Act).

4. Given widespread lock-in effects, users are over-exposed to uncontrolled raises in subscription fees by vendors, the payments of which put a recurring, never ending strain on public budgets. Examples are the ever rising subscription fees for Microsoft Office 365 and the usurious increases applied to VMware licence fees.

Especially for public administrations, the proprietary subscription model comes with an additional drawback: loss of accountability for administrative decisions by public bodies. Decision support systems are black boxes that undermine transparency and accountability.

Cut costs, gain freedom

In contrast, free and open source software is typically built on open standards and protocols that enable interoperability between products of different vendors and minimise the risk of vendor lock-in. While open source software can also be delivered through subscription models, this flexibility empowers public administrations and other users to better control costs by selecting vendors that are cheaper or offer better quality without compromise.

Wherever the respective FOSS licence allows, public bodies are also able to commission changes to the products they use to ensure that they meet the administration's needs. Those changes will only have to be paid-for once and can be reused forever without artificial licencing limitations. Free and open source software allows public administrations, for example, to co-develop software solutions, share technical expertise, and jointly maintain digital tools that are needed across the continent—without the need for every individual user to pay steep recurring licencing fees to a proprietary vendor. This approach reduces long-term costs and maximises the technological sovereignty required to remain operational in a world of geopolitical uncertainty.

This is already happening in some parts of Europe, with coordination and collaboration facilitated by the European Commission's own Open Source Observatory. It is also most recently being showcased by the multi-country collaboration around the German OpenDesk and the French La Suite projects for a joint European digital workspace. These efforts should be substantially scaled up in order to benefit more and more public authorities and thereby increase the EU's digital resilience.

Transparency, reproducibility, and auditability

Free and open source software not only provides for the availability of source code, as discussed above. If done well, it also offers the possibility for professional users to reproduce the source code bit by bit. Reproducibility of software code can guarantee that the application deployed on users' devices is, in fact, built with the exact same source code that has been made available by a vendor.

Code reproducibility is an essential tool for reliable digital security guarantees as well as professional auditing and transparency. That is why security-sensitive software vendors in particular have been striving to enable code reproducibility for their products. In proprietary software products, transparency, reproducibility, and auditability are hard or even impossible for public administrations to achieve.

Contribute to the digital commons

By engaging in the use, development, and maintenance of free and open source software, public administrations have the chance to turn a mere spending item in their IT budgets into a public interest investment with positive returns for society. Every bit of code that is published under a FOSS licence has the potential to contribute to Europe's digital commons, a body of works that is crucial for society and can be used, shared, studied, and improved by anybody else.

Well-established examples of digital commons that have a major positive impact on digital innovation are:

- The Wikipedia encyclopedia that has become the largest in history;
- The global mapping programme OpenStreetMap that is built into commercial map products, and used by individual users and by some of the largest companies alike;
- The Linux operating system is the most widely used operating system today. Because of its FOSS licence and its versatility, it powers billions of Android smartphones globally as well as the large majority of server farms on the internet.
- Nginx and the Apache HTTP Server are highly popular web server applications, together serving around 60% of all websites today.

What these examples have in common is how their governance is often rooted in democratic practice, with shared ownership, and a baked-in resilience against centralised (private or state) management of technology and towards democratisation of digital infrastructure and power. Investing in Europe's digital commons therefore strengthens our resilience not only against dependencies from Big Tech, but also against political vulnerability vis-à-vis rogue foreign governments that abuse their national software industry for political blackmail.

The EU has already taken timid steps to contributing to the digital commons, each of which has added tremendous value to the digital commons in Europe:

- In 2014, the European Commission launched the EU-FOSSA project (Free and Open Source Software Auditing), aimed at increasing the security and integrity of critical open source software applications used by the EU institutions.
- Since 2018, the EU's Next Generation Internet (NGI) initiative has funded over 1,000 Free and Open Source Software applications through cascading funding, most notably via the NGI Zero consortium. This public contribution directly strengthened the European open

source sector, including core pieces of the European technology stack.

- In 2020, the European Commission has founded the EC Open Source Programme Office (EC OSPO) as a "first concrete action of the latest Open Source Software Strategy for 2020-2023." It acts as a "facilitator for activities outlined in the strategy and the action plan," according to its own website.
- In 2021, the European Commission has launched FOSSEPS - Free and Open Source Software Solutions for European Public Services, an initiative to share knowledge and enable collaboration. The initiative identified critical open source software projects, to which it recommended that European public services should actively contribute to their long-term sustainability.
- In 2025, the European Commission has approved the creation of the Digital Commons EDIC (European Digital Infrastructure Consortium), an EU instrument enabling Member States to jointly develop, deploy, and operate cross-border digital infrastructures, with a dedicated governance and legal personality.

Today, it is essential for the EU to follow up on those first steps and substantially increase public investments in the further development of the digital commons in order to save public spending in the long-term, to reduce geopolitical risk through technological dependencies, to prevent vendor lock-in, and increase digital security for all in Europe.

3. What concrete measures and actions may be taken at EU level to support the development and growth of the EU open-source sector and contribute to the EU's technological sovereignty and cybersecurity agenda?

First, the EU should make the free and open source principle a requirement for the public procurement of software products and services. This would provide a massive boost to Europe's open source sector without spending any extra resources. It would also signal to the market the value of open source and help increase the overall transparency and trustworthiness of software production globally. It should also resolve the persistent perceived lack of clarity regarding governmental bodies developing and releasing open source software and its relationship to state-aid rules.

Second, the EU should establish a permanent European Digital Commons and Infrastructure Fund (others prefer to call it "Digital Sovereignty Fund") tasked to provide sufficient and reliable financial support to the development of the digital commons, including strategic free and open source software and open standards that contribute to the digital commons: Examples are the development of core internet infrastructure, an open browser engine, an independent search index, an open source mobile operating system, a decentralised and secure messaging protocol, decentralised social media software, and similar key building blocks that directly increase the digital self-determination of people, organisations, and companies in Europe. Much of these digital building blocks already exist today, but are chronically underfunded.

It is crucial that such a Fund is not exposed to political influence. It should instead be independently governed or arranged with one or several trustworthy, independent outside parties that work in the public interest, such as the Sovereign Tech Agency or the NLnet Foundation, which has managed NGI funds. The process should be transparent and involve all affected stakeholders, including civil society, software developers, public interest foundations and, where involved in the development, industry.

Third, the EU should adhere to the Public Money Public Code principle: Any software code funded by public money in the EU must be made available to the public under a free and open source software licence. This would minimise the risk of public funds being spent over and over by all the different public administrations to develop the same kind of software that already exists elsewhere in Europe. In the age of AI and other automated decision-making in public administrations, this would also increase transparency and public trust in the technology used by authorities.

WHAT NEEDS TO BE DONE

4. *What technology areas should be prioritised and why?*

Predicting which technological areas are going to be important in the future can be difficult (see e.g. failed hypes like blockchain, the metaverse, and "Web 4.0"). Political institutions like the European Commission are probably better positioned to facilitate and make available funding for technological ecosystems instead of to direct or select them, which should be done by independent parties or public interest foundations.

It is, however, essential to acknowledge that in the current geopolitical context, the EU should focus its resources on obtaining a higher degree of digital self-determination in technology areas that are critical for the functioning of its digitised economy *today*. That means we should focus on established applications and infrastructure that has already become irreplaceable, rather than on potential future innovations that may or may not become important. Hence, as impressive and exciting as the capabilities of some of the newly developed large language models and artificial image generators ("generative AI") might seem, they cannot be counted as critical infrastructure (yet). An objective assessment must conclude that the following digital applications and infrastructure are substantially more critical for the functioning of our current society and economy:

First, the fundament of many internet-connected technologies is cloud infrastructure. The availability of trusted, scalable, and globally distributed storage and computing power ("hyperscalers") is a key asset for Europe's capability to build and reliably deploy digitally sovereign online applications of all kinds. The EU should therefore apply a multipronged strategy that translates the framework of the EU Data Act into action, beyond non-binding standard clauses, and that adds procurement best practices, interoperability standards and reference open source implementations to the mix.

This should be more of a fast-follower strategy than of predicting an inherently uncertain future, for example through micro-grants for open source implementations of cloud APIs. These APIs are not magic, but their inherent infrastructural nature makes them less attractive for commercial parties to implement. A rare example of this already having happened are the reimplementations of Amazon's S3 API. Making open source implementation of the hyperscaler APIs available would considerably reduce vendor lock-in.

Second, one of the most central pieces of the digital commons is what is often referred to as the 'digital public town square,' a title regularly claimed by commercial social media companies. A public town square forms an essential piece of democratic infrastructure for a society to hold public debate and form opinions independently. The same is true in the digital world.

Commercial social media platforms such as X, Facebook, Instagram, or Threads, however, are not driven by an incentive to build and maintain a public town square and foster democratic debate and opinion shaping. They are driven by maximising advertising profits and therefore cannot fulfil the functions they claim to offer. Instead, they rather resemble private shopping malls whose owners are openly supporting authoritarian politics and the pursuit of undermining Europe's democracy and self-determination.

The digital public town square needs to be built and maintained by the public and for the public. Luckily, the work is already underway: Communities from around the world have built free and open source social media software on top of an open standard protocol (called ActivityPub) that is today used by millions of people. Examples include the micro-blogging application Mastodon—already used by the European Commission as well as Executive Vice-President Virkkunen—, the media sharing application Pixelfed, as well as the video sharing application Loops. Together with dozens of other compatible apps, they form a truly public town square for public debate unencumbered by ad-driven algorithms and other Big Tech interferences.

As free and open source tools, these applications owned by the public and as such should also be publicly funded. The EU and Member State governments should therefore not only start supporting this global social network by using it, but also by substantially increase the funding for its development and maintenance. This includes funding of the stewardship of the underlying open standards.

Third, much of today's digital markets and applications are mobile first. Many public and commercial services encourage or even require the use of smartphones: e.g. for buying and holding tickets, for payments, authentication, and other government services. Yet, this global

€500+ billion market is firmly in the hand of only two US-based tech companies: Google and Apple. This market duopoly creates enormous downsides for consumers, business users, and public administrations in the form of lack of choice, built-in massive data extraction, and data security risks. The deep integration of mobile devices into our societies makes our level of dependency to these two Big Tech companies particularly problematic. Today, every mobile application, no matter how sovereign or European, depends on being compatible with Apple iOS or Google Android operating systems. And it can be rejected and removed from dominant app stores by those two companies at any time, for any reason, or for no reason at all.

The EU should therefore start supporting the (already existing) development of alternative open source mobile operating systems—some of which are based on the Android Open Source Project and some are entirely independent. This is a major undertaking that will take years. But it can build on the excellent work that has already been done by the open source community and European and other non-US companies. This must be seen as a foundational element in any open source strategy that aims to boost Europe's digital sovereignty.

EU institutions and national governments should also take additional steps to ensure that all government issued software applications are available to users through channels independent of dominant Big Tech companies, for example by publishing them in alternative app stores and by making them downloadable from the web (sometimes referred to as "side-loading"). This measure would be consistent with and in support of the Digital Markets Act's requirement for gatekeepers to allow people to use third-party app stores.

Fourth, despite the strong pivot of most Big Tech firms towards AI chatbots and their aggressive integration into the most dominant search engines, the ability to index and search the Web without interference, censorship, or surveillance remains a strategic capability for any society. There are a number of search engine competitors, but Google has established itself as a quasi-monopolist in most countries and controls by far the world's largest search index. Due to the high development costs and technical complexity of building an index of that size, most search engine competitors do not have their own but effectively buy access to Google's or Microsoft's (Bing) search index.

This creates a dangerous concentration of power in the hands of two companies who control who gets access to which part of the index and how billions of people find and obtain access to online content. That is why the EU's open source strategy should provide stronger support for projects that are already building a public-interest search index for Europe, such as OpenWebSearch. As part of the digital commons, such an index would be available for competitors, both commercial and non-profit, and provide the EU, its companies and public administrations with strategic and independent access to global search capabilities.

Fifth, the browser remains an essential software application as it constitutes every user's window to the World Wide Web. In other words: a company that controls the browser market, controls the way people see and use the Web. Today, there is at least some competition on the browser market, with a dominant position for Google Chrome and low market penetration by competitors like Mozilla Firefox, Apple Safari, Microsoft Edge, Vivaldi, Opera, and others.

What is striking though is that the large majority of all those browsers rely on a single dominant browser engine: Google's Blink. A browser engine is the core of the application that renders the websites, and there are currently only three relevant engines being used: Google's Blink (~75% market share in Europe), Apple's WebKit (~20%), and Mozilla's Gecko (~4%). Even Microsoft, a billion-dollar corporation and major Google competitor, has shelved its own browser engine and instead builds its Edge browser with Google's Blink. As a result, two US gatekeepers—Google and Apple—control how the world accesses and sees the Web. Mozilla as a non-profit foundation would theoretically be a strong candidate for shepherding an independent public interest browser engine. But the foundation depends, and has depended on for a long time, almost entirely on funding from Google in exchange for making Google the default search engine in the Firefox browser.

The EU should therefore strengthen its open source sector and boost people's digital self-determination by investing in the development of a public interest, free and open source browser engine that is independent of Big Tech and that can be adopted by competitors without risking commercial vassalage vis-à-vis Google or Apple. This could be done by either re-using Mozilla's existing Gecko engine and transferring ("forking") it into a public interest foundation that is independent of Google's advertising contribution, or by heavily supporting a new, sovereign browser engine such as Servo.

Sixth, the EU should join Member State governments in investing in the development and maintenance of an open, decentralised, and end-to-end encrypted messaging protocol. While there is some competition in the messaging app market, with the Signal Messenger leading the charge in terms of security, most professional communications still depends on Microsoft Teams, Google Meet, Zoom, Slack, and similar Big Tech applications, most of which are based in the US. Even Signal has to rely on US cloud infrastructure (see above on cloud infrastructure sovereignty). Due to valid security concerns, government agencies, militaries, and police forces have started implementing their own communications solutions based on the open source Matrix protocol. While this is a positive step, the protocol itself is being maintained and innovated upon by a tiny, chronically underfunded European non-profit foundation. This is not sustainable.

In addition to rolling out more such independent open source communications infrastructure, the EU should therefore start financially contributing to the protocol level as part of the European digital commons.

SUMMARY

Europe is at a crossroads. The new, painful geopolitical reality requires us to adapt quickly. The EU will not achieve digital self-determination and sovereignty by trying to replicate the predatory and harmful business models of Silicon Valley, which followed the "move fast and break things" mantra. We have broken enough things.

It is time for Europe to build a digital ecosystem that serves as counter-point and proves that technology can serve people and the planet. It is time for us to build sustainable, human-centred tech businesses instead of VC-fuelled start-ups designed to lock in users in order to sell out to Big Tech. It is time to support projects and companies that have baked in respect for EU law and fundamental rights.

Free and open source software, open standards, and community-led, transparent tech development and deployment, in particular in the public sector, are essential ingredients in this endeavour. They must be the cornerstones of the EU's digital sovereignty ambitions.

***