Tech Sovereignty Package, part 1: Europe’s decisive step in a global race?

The DeHavilland Guide

Tech Sovereignty Package, part 1: Europe's decisive step in a global race?

The DeHavilland Guide

Contents

Authors

Eleonora Bottin
Lead Policy Analyst

Tri Nguyen
Policy Analyst

Vlad Enasescu
Policy Analyst

Fakhria Al-Bidir
Lead Policy Analyst

Igor Sarkissian
Head of EU Policy and Service

Editorial team

Steve Tolley
Group Political Content Editor

/ Key takeaways

- The recent Tech Sovereignty Package marks a shift from regulating digital markets to actively building strategic capacity across cloud, AI, chips, open source, and energy-linked infrastructure.
- This is the first of two deep dive briefings on the package, and looks at how the Commission defines sovereignty, how the various parts of the package contribute to this, how it has been received, and where it risks coming up short.
- The package defines sovereignty not as technological isolation, but as "open strategic autonomy", preserving openness while reducing critical dependencies and exposure to foreign interference.
- CADA is the centrepiece, using public procurement and risk-based assurance levels to steer demand towards trusted cloud and AI services.
- The EU's cloud and AI approach is one of managed openness: non-EU providers can remain active in the market, but stricter safeguards apply to sensitive public-sector uses.
- The main test for CADA will be whether it changes procurement behaviour, or whether demand remains concentrated at lower assurance levels where incumbent non-EU providers can still qualify.
- Chips Act 2.0 seeks to correct the limits of its predecessor by moving from headline production targets towards a broader semiconductor ecosystem strategy, to address challenges not only in manufacturing capacity, but also design, software layers, packaging, equipment, industrial adoption, late-stage finance and sustained demand.
- The Open Source Strategy offers Europe a less protectionist route to sovereignty by reducing lock-in, improving auditability, and supporting reusable European digital building blocks.
- The energy roadmap shows that Europe's technology ambitions depend on access to affordable, reliable and clean electricity, as data centres, AI and chips become inseparable from grid capacity and energy planning.
- Reception to the package was mixed and there are risks of divisions within and between the co-legislators. There are also concerns that the package could not be enough to achieve independence from the US or China at the same time as risking damaging relations with Washington and Beijing.
- Part two of this briefing will look at how the regime the package will bring about compares with that of China and the US.

/ Europe and the global race for tech leadership

The Union's focus on competitiveness is a staple of the current mandate. The Commission has a clear objective to support the European economy and its ability to compete in increasingly adversarial global markets. This overarching objective has been intertwined with concerns over the Union's sovereignty, with a view to address overdependencies and supply chain risks.

The Commission has laid down plans and policy agendas to bolster sectors perceived as strategic and instrumental to sovereignty – such as the Industrial Accelerator Act or the Automotive Package. The adoption of the Tech Sovereignty Package on 3 June 2026 is another step in this process, and a key milestone in the Commission's ambition to position the EU as a leader in the development of new and frontier technologies.

> *"Europe has the talent, the research excellence, the industrial base and the Single Market. Together, we must turn these strengths into technological sovereignty"*
>
> Commission President Ursula von der Leyen

The Commission promises that this package will unshackle Europe's potential to lead in the sector. However, it does not exist in a vacuum, and other powers are already positioned in the race for technological leadership.

The United States, home to several global tech giants, has clear claims to hegemony in the sector. The recent capitalisation of SpaceX and the upcoming IPOs of OpenAI and Anthropic are testament to this aspiration. Similarly, China is home to the other tech giants and its domestic model DeepSeek and has set out clear ambitions to achieve autonomy while offering an alternative and competing ecosystem.

Beyond ambitions and discourse, all competitors in this global race need to create policy, and economic and governance frameworks that can deliver.

Part 1 of this briefing will go through the different elements announced in the Tech Sovereignty Package, looking at what they intend to do, how they have been received and where they could come up short.

Part 2 will then compare the resulting framework to American and Chinese initiatives to understand whether European is following through on its narrative.

Package breakdown & analysis

How the package defines sovereignty

The EU's Tech Sovereignty Package does not present sovereignty as a call to build a closed, Europe-only technology ecosystem. Instead, it defines it as the ability to keep control over the technologies, infrastructure, services, and data that are essential for Europe. The aim is to reduce excessive dependencies and exposure to foreign interference, while allowing Europe to benefit from global markets, partnerships, and innovation. In other words, the package seeks to keep Europe open, but with enough capacity of its own to avoid being vulnerable.

The political fault line is therefore not simply "Europe first" versus "global openness". It is about which layers of the technology stack require European control, and which can safely be integrated in allied supply chains. The Commission rejects the idea that sovereignty equates to isolation, protectionism, or tech decoupling. Rather, the package presents openness as sustainable only if Europe has enough domestic capacity and diversified supply chains to prevent strategic dependencies from becoming vulnerabilities.

This logic is clearest in cloud and AI. The **Cloud and AI Development Act** (CADA) treats compute infrastructure as a strategic resource. Europe's limited data-centre capacity and dependence on a small number of third-country hyperscalers create risks for data access, operational continuity, and vulnerabilities to foreign jurisdiction. Its proposed sovereignty framework translates "sovereign" into auditable criteria: where infrastructure and data are located, who controls the provider, whether support and personnel are in the Union, how software supply chains are secured, and whether public-sector use cases require higher assurance levels. For sensitive public functions, sovereignty therefore means not only cybersecurity, but also operational and legal autonomy.

The **Chips Act 2.0** applies the same reasoning to semiconductors. The problem it aims to solve is overdependence on third countries for design and manufacturing: the EU produces less than 10% of global semiconductors and is almost entirely dependent on the US and Asia for leading-edge chips below 5 nanometres, including AI chips. The response is to build more European capacity across the supply chain, while remaining open and cooperative.

Open source is the package's bridge between control and openness. The **Open Source Strategy** presents transparent, verifiable, and reusable software to reduce lock-in and build European alternatives without retreating into isolation. In this sense, "sovereign" does not always mean proprietary or nationally controlled. It can also mean portable, inspectable, community-governed, and less dependent on a single vendor.

Overall, the package defines sovereign technology as technology that Europe can trust, govern, sustain and substitute if necessary. The compromise is "open strategic autonomy": control over critical layers, diversification of risky dependencies, and openness where partnerships strengthen resilience rather than deepen dependence.

CADA: Europe's enablement crown jewel

CADA is a central piece of Europe's response to sovereignty and competitiveness concerns. The EU remains structurally dependent on non-EU providers for a large share of its digital products, services, and infrastructures. CADA seeks to address this situation by making public-sector demand a central lever of the EU's sovereignty agenda.

Importantly, CADA should not be read as a blanket data localisation regime or a ban on third-country cloud and AI providers. It is instead a risk-tiered sovereignty framework that uses public procurement, assurance levels, and risk assessments to steer demand towards more trusted cloud and AI services. The central question is therefore not whether non-EU providers will be excluded from the European market, but whether the framework will meaningfully reduce strategic dependencies or whether most procurement will remain at lower assurance levels where existing non-EU providers can still qualify.

Balancing market development and security

The proposal's focus is public-sector procurement. Public administrations would be required to assess the sensitivity of cloud and AI services they procure and apply one of four sovereignty assurance levels based on criteria relating to establishment, control, infrastructure, staffing, data location, subcontracting and the use of data for AI training (see boxout). Levels 3 and 4 are designed for more sensitive public-sector uses. They introduce stricter requirements on personnel, control, subcontracting and supply chains.

SOVEREIGNTY ASSURANCE LEVELS	
Level 1	Likely to cover a large part of ordinary public-sector procurement, Level 1 requires, among other things, that the provider be established in the EU and that customer data remain in the EU, while still allowing non-EU subcontracting under certain transparency conditions.
Level 2	Adds stricter requirements, including around subcontractors and restrictions on the use of service-generated data for third-country AI systems. At this level, foreign control may still be possible if it cannot compromise the service.
Level 3	Limits third-country control, although trusted partner countries may still be treated differently. This sovereignty level requires the personnel to be EU citizens (and not just EU-based). Third-country control over the provider and relevant subcontractors is not allowed in most cases, except in the case of trusted partner countries.
Level 4	Conditions could be so strict that they will only affect highly sensitive cases (e.g., defence-related activities). Conditions include the requirement for the highest cybersecurity certificate and no third-country control whatsoever in the software supply chain.

Beyond the public sector, the framework has implications for strategic sectors covered by NIS2 (e.g., finance, energy, healthcare, transport, and telecommunications). The inclusion of private entities is targeted and risk-based rather than a general extension of public procurement rules to the private sector.

The framework does not aim to displace US hyperscalers from the European public sector market. Rather, it defines the conditions under which they may participate, reserving the most sensitive activities for providers that meet high sovereignty requirements.

This approach represents a concrete attempt to reduce Europe's reliance on third countries for cloud and AI computing services. The proposal's provisions on faster permitting and grid connections for data centres could also support the development of physical AI infrastructure in Europe.

All told, CADA reflects a broader shift in the Commission's approach: from regulating digital markets through obligations and restrictions, towards actively building technological capacity. The "Free Software first" requirement could also help reduce vendor lock-in and create more opportunities for European SMEs.

Strategic step or stumble?

The framework also raises important questions. Levels 3 and 4 may create market access and scaling barriers for providers seeking to compete for sensitive public-sector contracts. Some companies may find it difficult or costly to meet criteria based on ownership, control, personnel and supply-chain conditions. This may limit provider's ability to access high-sensitivity public contracts unless they adapt their governance and operational structures.

The key policy question is whether enough public-sector demand will move towards higher assurance levels to help European sovereign cloud providers scale, or whether most demand will remain concentrated at levels 1 and 2, where established non-EU providers may still qualify.

As always in the EU, implementation will make or break the Commission's ambitions. Leaving sovereignty assessments to national authorities could produce divergent interpretations across Member States. Such fragmentation could weaken the overall objective and create uncertainty for providers trying to qualify across the EU. The proposal also appears to lack requirement for public authorities to assess credible European alternatives before procuring from a non-European provider. Without such a demand-side discipline, the framework may fall short of its sovereignty ambitions.

The proposal raises questions about how the EU intends to reconcile its AI and cloud ambitions with energy and sustainability concerns. Across the package, the Commission defines sustainability in digital infrastructure through energy and resource efficiency standards for data centres. New data centres may be required to meet higher efficiency benchmarks, but the broader environmental, social, and human rights implications of large-scale AI infrastructure receive less attention. The package is strongly pro-capacity: it treats cloud and AI infrastructure as strategic assets that Europe must build, while giving comparatively less weight to the risks associated with accelerating deployment.

CADA should therefore be understood as both a sovereignty instrument and an industrial policy tool. It responds directly to Europe's dependence on international partners for cloud and AI capabilities, but it does so through managed openness rather than outright protectionism. The proposal creates space for providers from trusted or associated partner countries to access higher assurance levels under certain conditions. This keeps the market relatively open to allied providers, while still allowing the EU to ring-fence the most sensitive uses.

This balance may become politically contentious. Some actors will argue that the framework is not ambitious enough because it does not create strong "Made in Europe" requirements for public technology spending. Others will argue that the origin and control criteria, especially at levels 3 and 4, are already too restrictive and could undermine openness, competition and transatlantic relations.

A mixed reception

Stakeholder reaction to CADA has been mixed. Its overall objective of reducing Europe's dependency on large non-EU cloud and AI providers has generally been welcomed, particularly by industrial stakeholders. Measures such as dependency mapping and faster permitting for data centres have been seen positively by organisations such as Orgalim and ASD, as they could help identify strategic vulnerabilities and accelerate the deployment of European digital infrastructure. However, support for the objective has not translated into full support for the proposal's design.

One recurring criticism is that CADA remains too focused on public-sector procurement and does not do enough to stimulate demand in the private sector. The European DIGITAL SME Alliance and Connect Europe have argued that a stronger demand-side push is needed if European cloud and AI providers are to scale beyond public administration. This echoes a broader concern with the proposal: procurement rules can help create a market for sovereign services, but they may not be sufficient if private companies in critical sectors continue to rely primarily on established non-EU providers.

Sustainability concerns have also featured prominently in stakeholder reactions. SGI Europe and Leitmotiv have warned against an "all-in" approach to AI infrastructure that treats the expansion of data centres and compute capacity as an unquestioned strategic objective. From this perspective, the package risks underestimating the climate and resource implications of accelerated AI uptake. While the proposal includes energy-efficiency requirements, critics argue that this does not fully address the broader environmental consequences of rapidly expanding Europe's digital infrastructure.

Civil society organisations have raised a different set of concerns. ARTICLE 19 described parts of the package as "sovereignty washing", warning that technological sovereignty could be used to justify deregulation in areas such as AI governance and data protection. It also criticised the fact that the strictest cybersecurity and data-transfer safeguards would apply only at the highest sovereignty levels. A similar concern was raised by CISPE.cloud, which argued that levels 1 and 2 may not go far enough and could leave structural loopholes in the framework. These criticisms point to a wider question: whether the lower assurance levels will create meaningful sovereignty safeguards or mainly provide a sovereignty label without substantially changing market behaviour.

There is a risk that the proposed criteria used to define sovereignty focus too heavily on geography and nationality. While jurisdiction and control are relevant, digital supply chains are global and complex. For stakeholder players such as ITI Council, BSA, AmCham EU, and CCIA Europe, a more effective approach would be to place greater emphasis on governance, operational resilience, transparency, risk management, auditability and enforceable control over critical functions. Otherwise, the EU may create a system that is formalistic without necessarily improving actual resilience.

Commission vision and political frictions

The proposal is likely to face difficult negotiations between the co-legislators, particularly on the design of the sovereignty assurance framework. In the European Parliament, several groups are expected to push for a more ambitious approach. The Greens/EFA have argued that, without clearer "Made in Europe" requirements for public tech spending, the EU may not achieve long-term independence from the US. Renew Europe has similarly called for stronger measures to increase both the development and uptake of European alternatives. The S&D group has also pointed to the US restrictions on access to advanced AI models as evidence of Europe's exposure to foreign governments and companies.

In the Council, Member States may be divided. Some governments may support a stronger sovereignty framework and a clearer preference for European providers. Others may be concerned that strict origin and control criteria could reduce competition, complicate procurement, or damage relations with key partners such as the United States. The fact that many decisions would be left to national authorities may also raise concerns about fragmentation and inconsistent application.

The recent Franco-German position paper shared at VivaTech gives some indication of where the debate may go in the Council. France and Germany appear to support a combination of defensive and proactive measures, while avoiding a fully protectionist approach. This suggests that the final compromise may preserve the basic structure of CADA, but adjust the balance between openness, trusted partnerships, and stricter sovereignty conditions. The main negotiation will therefore be about how much demand the EU is willing to reserve for genuinely sovereign European providers, and how far it is prepared to go in reshaping public-sector technology procurement.

Chips Act 2.0: bridging capability challenges

This proposal puts forward a revision of the EU Chips Act adopted in 2023 that had several shortcomings. It supported front-end manufacturing projects and research incentives but did not fully address structural weaknesses in Europe's semiconductor ecosystem. It lacked coordination mechanisms and integrations with sectoral policies (e.g., machinery, automotive, energy, or defence). As a result, it did not provide the value-chain-wide impact that was anticipated and left the EU in a vulnerable position in the semiconductor supply chain.

Righting a wrong

The EU remains heavily dependent on external partners, including the US and China, for critical technologies, materials, equipment and manufacturing capacity. Although Europe has world-class strengths in research, chip design, equipment, and industrial applications; it still produces less than 10% of global semiconductors. The original Chips Act set the target of raising the EU's share of global production to 20% by 2030 but meeting that objective requires more than attracting a few flagship fabs.

The Chips Act 2.0, seeks to build on the first iteration and address its weaknesses. The main shift is the stronger demand-side component. Rather than focusing only on production capacity and research, the proposal aims to create a more complete European semiconductor ecosystem. This responds to one of the main criticisms of the first Chips Act: that Europe has strong research and applied technology capabilities but struggled to translate them into industrial scale.

The Chips for Europe component intends to strengthen the industrial-capacity of the sector and bridge the gap between Europe's research strengths and its weaker manufacturing and deployment base. The "first-of-a-kind" framework would also be expanded beyond traditional fabs to cover a broader part of the semiconductor value chain. Expanding the policy's scope is intended to help develop sovereignty over the full spectrum of relevant activities – packaging, materials, equipment, design, industrial chips, and embedded systems – and connect semiconductor innovation to downstream demand.

Creating conditions to solve dependencies

The proposal seeks to address vulnerabilities linked to third-country dependencies. It clearly sets out that public support and strategic projects should not deepen Europe's exposure to actors whose involvement would be incompatible with EU security or strategic autonomy interests. Instead of creating a blanket exclusion regime, the framework appears to rely on justification, risk assessment, and compatibility with EU interests. The scope of those measures is likely to be one of the volatile elements in the work of the co-legislators.

Permitting is another key element of the proposal. Semiconductor projects are capital-intensive and time-sensitive, and Europe has often been criticised for slow approval processes. A stronger fast-track permitting system could therefore help reduce delays and make the EU more attractive for industrial investment. However, faster permitting alone will not be able to bolster attractiveness and Europe needs to provide sufficient infrastructure, energy access, skilled workers and long-term demand if it wants to become more attractive.

The financing challenge is even larger. The Commission estimates Europe will require an additional €120 billion in public and private investment for the semiconductor industry by 2035. To support this, Chips 2.0 includes a Chips Fund operated through instruments such as the EIC Accelerator, InvestEU, and public-private co-financing. A significant share of the funding would be directed towards a Union-based semiconductor foundry. The proposal also recognises that Europe's venture capital ecosystem is often insufficient for semiconductor scale-up, where costs are high, timelines are long, and commercialisation requires patient industrial capital. Funding is therefore expected to shift more towards scale-ups, later-stage financing, and deployment across priority industries.

Will Chips 2.0 convince the private sector?

The emphasis on large-scale supply-side capacity raises an important question: is this where Europe is best placed to compete? Building cutting-edge semiconductor manufacturing capacity is expensive, while production costs in Europe remain higher than in leading Asian markets. Some stakeholders argue that the EU should focus less on catching up in every segment of the global race and more on scaling the areas where it already has comparative advantages. Europe is already home to innovative chip technologies for industrial, automotive, energy, and specialised applications. A strategy focused on scaling these strengths may be more realistic than trying to replicate the full supply-side model of Taiwan, South Korea, China, or the United States.

This concern is particularly relevant to the proposal's focus on cutting-edge sub-2nm logic chips. While advanced-node capacity is strategically important, it is not obvious that Europe has sufficient industrial demand or consumer willingness to sustain expensive projects at scale. Chips "made in Europe" may be politically attractive, but end users may not be willing to pay a premium for European origin alone unless it is linked to security, reliability, performance, or regulatory requirements.

The Demand Forum and Demand Accelerators are meant to address this problem. They could help aggregate demand across sectors, connect semiconductor producers with downstream industries, and reduce the fragmentation that limited the first Chips Act. This is one of the most important elements of the proposal. If it works, Chips 2.0 could move EU semiconductor policy away from isolated flagship projects and towards a more integrated industrial ecosystem. If it fails, Europe risks financing expensive capacity without ensuring European companies use it.

There is also a risk funding remains strongest at the early stages of innovation, at the expense of the later stages of scaling and industrial deployment. This was one of the weaknesses of the first Chips Act. Although the headline figure was €43 billion in public and private investment, the Commission's direct contribution amounted to only €3.3 billion, or around 7.7% of the total. By contrast, the US CHIPS and Science Act has been more effective at mobilising large-scale public support and approving state aid for major projects. Unless Chips Act 2.0 comes with clearer and more credible long-term funding commitments, Europe may again struggle to move from ambition to execution.

Chips Act 2.0 should therefore be understood as an attempt to move Europe's semiconductor strategy from a production target to an ecosystem strategy. Its central promise is not simply to increase Europe's global production share, but to make semiconductor policy more connected to users, markets, and security needs. The main risk is that the EU again focuses too heavily on headline capacity and not enough on adoption, scale-up, and industrial integration. Europe will only reduce its semiconductor dependency if it can create both supply and demand for European technologies.

Stakeholder supportive of objectives, with concerns over design

Stakeholder reactions to Chips Act 2.0 have been broadly supportive of the objective, but more cautious on the design. The proposal's aim of strengthening Europe's semiconductor ecosystem and improving supply-chain resilience has been welcomed by organisations such as ASD. However, as with CADA, stakeholders raised concerns about whether the proposal does enough to create demand and whether it focuses on the right parts of the value chain.

Orgalim has been particularly critical of the strong emphasis on sub-2nm logic chips. It says that while advanced-node capacity is strategically important, this focus may overshadow other advanced semiconductor technologies where Europe already has stronger capabilities, such as neuromorphic chips, photonics, and quantum chips. Orgalim adds that these areas could become European strengths if they are scaled effectively and that there is uncertainty over whether there is enough European market demand for sub-2nm logic chips to justify the launch of a costly foundry. It also warns that Europe could invest heavily in catching up with global competitors in the most capital-intensive segment of the market, rather than scaling the technologies where it may already have a comparative advantage.

At the same time, stakeholders recognise that Chips Act 2.0 does attempt to correct one of the main weaknesses of the 2023 Chips Act: the lack of a convincing demand-side strategy. TechUK has pointed to the proposal's focus on increasing the uptake of semiconductors designed or manufactured in the Union, particularly in sectors such as cloud, automotive, aeronautics, telecommunications, and defence. VDMA has similarly welcomed the broader inclusion of user industries, noting sectors such as machinery felt insufficiently integrated into the first Chips Act. This wider industrial scope could help connect semiconductor policy more directly to European manufacturing demand.

The question is whether these measures will be enough to compete with the US and China. Bruegel noted that Europe still lacks AI chip designers of global significance and does not have software layers comparable to CUDA or CANN. This matters because semiconductor sovereignty is not only about manufacturing capacity. It also depends on design capabilities, developer ecosystems, software integration, and downstream adoption. As long as Europe remains dependent on international competitors for key parts of the AI chip stack, it will struggle to build a fully domestic semiconductor ecosystem.

Open source: enabling for Europe's tech

The EU Open Source Strategy is the software layer of the package. It was framed as a response to a clear dependency problem: Europe relies heavily on non-EU providers across software, cloud, AI, and infrastructure. The Commission argues open source can give public administrations, businesses, and citizens more control, lower lock-in, stronger auditability, and reusable building blocks. It also positions open source as a facilitator to implement other EU initiatives (e.g., the AI Continent Action Plan, the Interoperable Europe Act, CADA, and the EUDI framework).

With 3 million open-source contributors already active in Europe, the strategy's central question is not whether open source is valuable in principle, but whether it can be turned into maintained, secure, and widely adopted infrastructure. The strategy treats open source as a capacity instrument that can support both sides of the market by facilitating emergence of new solutions, and their uptake.

The strategy is built around four objectives:

- supporting open-source alternatives aligned with EU values
- strengthening the European open-source ecosystem
- increasing open-source use in public administration, and
- linking open source more closely to standards and international outreach.

The Commission believes that open-source building blocks can reduce dependencies and create alternatives across technology ecosystems (e.g., internet stack, cloud, AI, cybersecurity, etc.)

Openness and sovereignty dilemma

The role given to open source creates a natural dilemma with broader sovereignty objectives. Open source tech stacks are by essence built collaboratively and iteratively by a galaxy of actors building upon existing tech stacks. Hence, with its reliance on collaboration and a complex global network of architecture and processes, open source does not automatically create European capacity.

The strategy acknowledges this tension by emphasising the role of scaling, deployment, maintenance, and governance in supporting the emergence of EU-grown open source tech stacks. It also gives the EU a less restrictive route to sovereignty than origin-based localisation. These technologies can support European control without requiring a fully European-owned stack at every layer. The strategy aims to embed Europe in global communities, standards, and reusable software while reducing dependence on closed systems. This approach is consistent with the model of 'open strategic autonomy' by setting objectives on the creation of more European capacity and choice, without full decoupling from global technology ecosystems.

Whereas open source can reduce lock-in, it does not automatically reduce dependency on hyperscalers, dominant developer platforms, AI infrastructure providers, or commercial support ecosystems. Open source could improve EU's contestability, but only if combined with procurement discipline, competition enforcement, funding, and migration capacity.

Driving open-source adoption

The most important demand-side lever presented in the strategy relies on public procurement. It aims to make public administrations users of open-source solutions through procurement guidance, open-source-friendly tendering, stronger Open Source Programme Offices (OSPOs), reusable digital solutions, and openness-by-design in digital investment decisions. This demand logic also extends beyond procurement: the EU's emerging digital identity ecosystem is itself being built around open, reusable components.

This strategy intersects with existing and potentially upcoming policy initiatives. The EUDI Wallet is a fitting example, as its reference implementation is made available through open-source code libraries, modular components, and a functioning reference application. This means open source is not only something the EU wants public administrations to buy, but it is also part of the infrastructure through which the EU is building common digital identity services. The European Business Wallet initiative is likely to become another piece of this puzzle. Digital identity may become one of the first large-scale tests of whether open source can move from policy preference to operational European infrastructure.

In the current European context, public buyers often may lack technical capacity to implement these objectives, and their risk-averse nature may deter them from procuring non-proprietary products from large vendors. For open source to become a real sovereignty tool, procurement rules need to reward long-term control, interoperability, auditability, reuse, and maintainability, not only upfront price or vendor reputation.

Open source's inherent weaknesses

The strategy recognises maintenance as a sovereignty issue. Critical open source components are often maintained by small teams, volunteers, or underfunded organisations despite being embedded in major public and private systems. The proposed Open Source Maintenance Instrument, critical dependency mapping, mirroring capabilities, security baselines, and stewardship support are therefore central to the package's credibility.

Funding remains an open question. The EU aims to mobilise around €2 billion over seven years for all measures under the Open Source Strategy, including the maintenance instrument, but stakeholders have already noted this is not much compared with Europe's estimated annual proprietary IT spend. FSFE puts EU spending on mainly proprietary IT products and services at around €264 billion per year, underlining the scale of the market the strategy is trying to shift. This creates a potential mismatch, since without sustained maintenance funding, open-source adoption could create new sustainability risks: public administrations may rely on open components that are transparent but not adequately maintained, secured, or supported.

Politically, open source can become shorthand for "good" digital policy without changing the underlying power structure of digital markets. It can improve auditability and reuse, but still rely on unpaid labour, weak governance, low adoption, and infrastructure controlled by dominant firms. The challenge for the EU is therefore not only to publish or procure more open-source software, but to build the institutional capacity around it.

Open source: what about civil society?

The open-source community has broadly welcomed the strategy as a breakthrough. Mastodon welcomed the Commission's decision to place open source at the centre of tech sovereignty, arguing that transparency, auditability, and decentralised technology can reduce proprietary lock-in and increase real control. OpenForum Europe framed the strategy as Europe's first comprehensive open-source framework and a recognition of open source as a horizontal enabler of structural sovereignty.

Large technology industry groups raised concerns regarding the way the EU intends to shape the choice of technology. ITI supported open source as a driver of global collaboration and innovation, but stressed that real-world digital ecosystems rely on both open-source and proprietary technologies. It also emphasised that organisations need flexibility to choose the tools that best meet their needs. BSA made a similar argument in relation to the wider package, warning against procurement rules that favour specific technologies or supply chains rather than objective security and resilience outcomes.

SME voices also focused on demand, as European DIGITAL SME Alliance's response to the wider package argued that supply-side investments must be matched by demand-side measures if Europe wants to scale homegrown technology providers. In the context of open-source systems, the organisation argued that Europe may have credible projects and companies, but without public and private adoption, these could remain niche alternatives rather than scaled infrastructure. Therefore, procurement guidance, tendering rules, OSPOs development, public-sector migration support and standards work will determine whether open-source providers, integrators, SMEs and steward organisations can turn political directions into market demand. Therefore, procurement guidance, tendering rules, OSPOs development, public-sector migration support and standards work will determine whether open-source providers, integrators, SMEs and steward organisations can turn political directions into market demand.

OpenForum Europe welcomed the Open Source Maintenance Instrument as a response to the market failure around maintenance. The Free Software Foundation Europe (FSFE) similarly sees the strategy as a potential milestone for the "Public Money? Public Code!" principle, but argues that implementation will depend on binding rules, secure funding, and civil-society involvement.

The open question is whether Europe can turn open source from a value statement into a capacity strategy. Open source could become one of the most practical parts of the Tech Sovereignty Package. However, if the EU fails to close the loop between funding, maintenance, procurement, and adoption, it risks remaining a non-binding signal of intent: useful for showing Europe's preferred model of technological approach and tech diplomacy, but insufficient to reduce dependence on the proprietary platforms and infrastructure that still shape much of Europe's digital economy.

Energy: plugging in Europe's tech ambitions

The last piece of the tech sovereignty puzzle is the EU's Strategic Roadmap for Digitalisation and AI in the Energy Sector. Rather than being a legislative initiative, the roadmap sets the direction for future EU action to reconcile energy and technology priorities by coordinating existing initiatives and announcing possible legislative, regulatory and funding measures.

In the roadmap, sovereignty is not presented only as producing or owning technology in Europe. It is more about being able to control, secure, and shape the digital tools, AI models, data flows and infrastructure that the energy system will increasingly depend on. This includes trusted access to technology, interoperability, data governance, cybersecurity, resilience, sustainability, and lower exposure to strategic dependencies.

Powering Europe's ambitions

The roadmap has several strengths. First, it includes funding and innovation support through Horizon Europe, AI Factories, testing facilities, scale-up instruments, and research calls for AI in energy. However, the EU's financial model is spread across different instruments rather than built around one large subsidy programme. This could make the approach more targeted, because funding is linked to EU priorities such as sustainability, interoperability, and security. At the same time, it raises a question of scale. The EU may have the right policy architecture, but not necessarily the same financial firepower or speed as the US or China.

A second strength is that the roadmap treats supply-side capacity as both an energy and a digital challenge. On the energy side, data centres are not seen only as digital infrastructure, but also as major electricity users that require grid access, stable supply, clean power, flexibility solutions, water management, and waste heat reuse. The proposed tripartite agreements between public authorities, data centre operators, and energy actors aim to support this integration by improving grid planning, clean energy sourcing, flexible connection agreements, energy performance, and water-resource protection.

The roadmap's approach is consistent with other EU initiatives in this field such as the rules on data centres reporting under the Energy Efficiency Directive and the data centre rating scheme under the European Grids Package. Indeed, the roadmap links digital sovereignty to the clean energy transition, aiming to make AI and data centre growth compatible with decarbonisation, affordability, grid stability, and environmental protection.

The digital side is equally important. The roadmap links sovereignty to the availability of compute, cloud, and edge infrastructure, smart grids, smart meters, data spaces, and secure connectivity. It addresses these needs through smart grid indicators, faster smart meter rollout, digital twins, AI models for grid management, and cross-border energy data exchange. This matters because digital ambition alone is not enough as it also depends on grid capacity, affordable energy, and reliable connectivity.

Third, the EU tries to create demand through regulation and market design, rather than through simple domestic preference. Smart meters, demand response, bidirectional charging, energy data hubs, and AI tools for grid management are expected to create users and buyers for trusted digital energy solutions. The risk is that technologies are developed but not actually used. The EU therefore needs procurement, consumer incentives, good tariff design and stronger capacity among grid operators and public authorities to turn supply into real adoption.

Return to contents page

Blind corners

There are also important limiters. The first is strategic dependency. The roadmap aims to reduce reliance on third-country digital tools, AI models, cloud providers, and critical components, especially where these create risks linked to espionage, cyberattacks, extraterritorial access, or supply disruption. However, important dependencies would remain, especially in advanced chips, GPUs, hyperscale cloud infrastructure, and some critical energy devices.

A second limiter is regulatory attractiveness. EU standards, reporting obligations, sustainability requirements, and cybersecurity rules can create trust, environmental accountability, and resilience, but they can also increase compliance costs. Data centre operators and investors may compare the EU with places where permitting is faster, energy is cheaper, and regulation is lighter. For this reason, the EU needs to combine regulatory ambition with practical administrative simplification, without weakening environmental and energy-system safeguards.

A third limiter is sustainability and resource pressure, including energy costs. Data centres use a lot of electricity, and energy is one of their largest operating costs. High or unstable electricity prices could make the EU less attractive for AI infrastructure. At the same time, the issue is not only industrial competitiveness. Data-centre growth can also create wider public-interest concerns such as grid congestion, higher pressure on electricity systems, water use, land availability, environmental permitting and maintenance capacity may all limit delivery. The EU's response, including clean power purchase agreements, co-located generation, flexible connections, waste heat reuse, and efficiency standards is distinctive because it tries to balance competitiveness with environmental and system-level constraints. However, it will be difficult to implement evenly across Member States.

Fragmentation is another risk. Energy regulation, grid planning, data access and smart meter rollout differ across Member States. If national approaches diverge too much, the EU may fail to create a real Single Market for smart energy services and AI-enabled energy tools. This would weaken the scale effect that is central to EU technology sovereignty.

Taken together, these elements point to a model of technology sovereignty that is both regulatory and infrastructural. The roadmap's main strength is that it links AI, data, energy, grids, cybersecurity, affordability and sustainability in one framework. The main challenge is implementation. The EU will need to turn rules and coordination into deployment by financing, building, connecting and adopting trusted technologies quickly, while keeping digital infrastructure growth compatible with its climate, energy and environmental objectives.

helio DeHavilland

We hope you found this briefing helpful.

This briefing is an example of the in-depth political information we provide to public affairs and policy clients every day.

Our analysts gather vital political content from a range of sources to bring our customers live coverage tailored to their strategic needs.

To find out how DeHavilland's political monitoring and research can help your organisation, and to request a consultation, visit our website: dehavillandeurope.eu