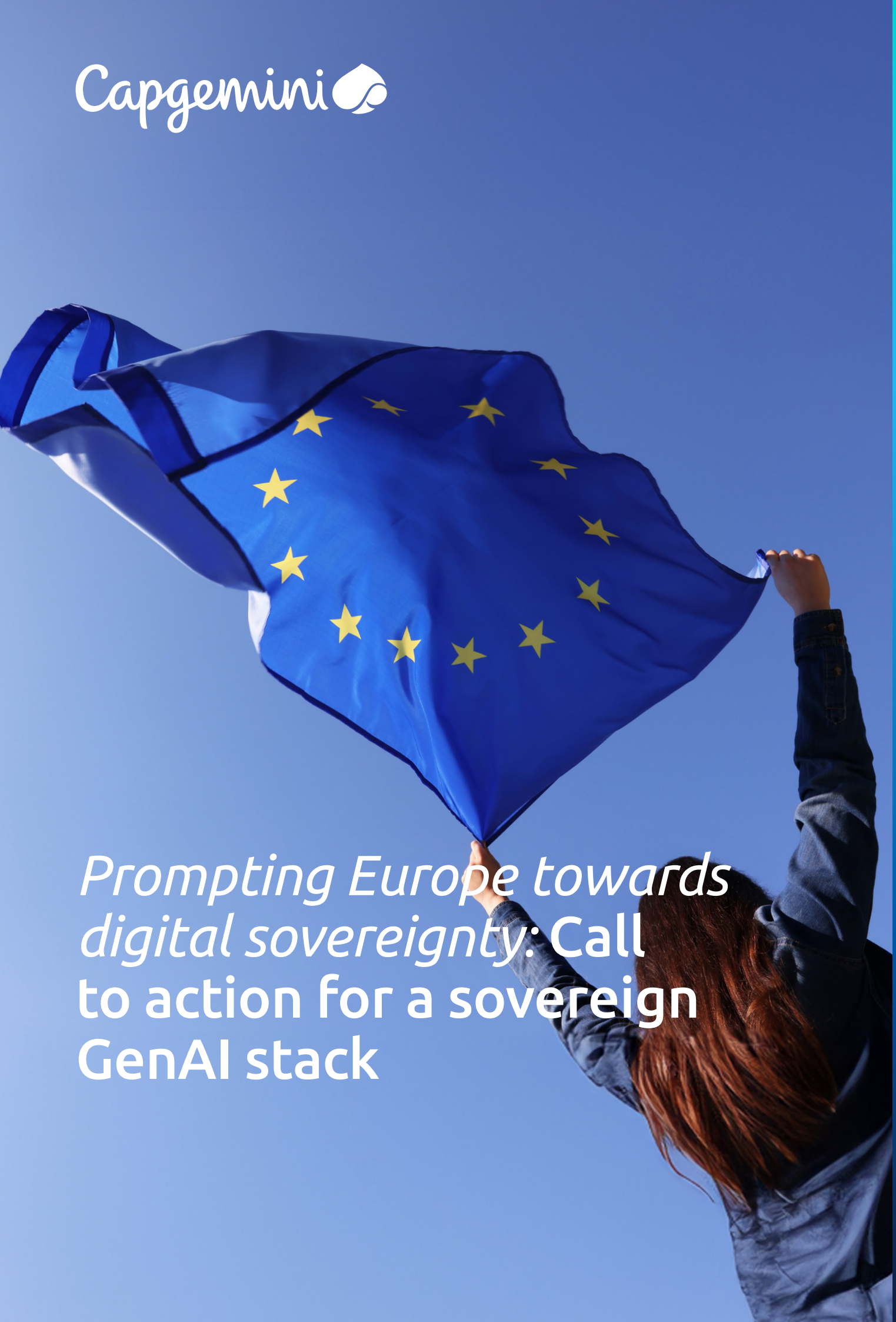
Capgemini



Prompting Europe towards digital sovereignty: Call to action for a sovereign GenAI stack

Table of contents

01

Digital sovereignty: Understanding what it is and why it is critically important today

"A European AI is essential for our future independence"

Ursula von der Leyen in her 2025 State of the Union Adress[1]

[1] *State of the Union 2025 - European Commission*

1.1 The GenAI balancing act

In full swing, the global digital transformation poses major challenges to many industries but also offers major opportunities – especially with the advent of generative artificial intelligence (GenAI) technologies. Getting the right balance between these opportunities and challenges is key to success going forward, and digital sovereignty will play a vital role in this balancing act.

For the public sector, GenAI offers the potential to revolutionize citizen services for the better – a desire shared by both public servants and citizens alike. GenAI can help meet a general need for more efficient public services and better user experience. For example, with the support of Capgemini, the Generalitat de Catalunya has introduced Generative AI to respond to citizen queries in Catalan, the local language, thus supporting a smoother and more inclusive experience for its citizens[2].

1.2 Emergence of new risk

However, in tandem with the opportunities afforded by GenAI comes a new level of risk pertaining to sovereignty. Thus, it is no surprise that the topic of digital sovereignty has taken center stage. This risk lies in the fact that the increased adoption of GenAI is occurring in an international environment marked by heightened tensions between global powers and changing international partnerships.

This difficult geopolitical environment has highlighted the risks inherent in countries' lack of control over their digital trajectories. Indeed, antagonistic actors may leverage their digital capabilities to others' detriment through surveillance, cyberattacks or other interventions, specifically targeting the public sector to undermine citizens' trust in their governments and fragment social cohesion. For instance, GenAI has raised cybersecurity risks, e.g., through more sophisticated attacks from a broader range of adversaries, a widening of organizations' surfaces for cyber-attacks or new vulnerabilities related to the use of GenAI for code generation[3].

Finally, given that most LLMs are developed in a very small subset of countries and trained disproportionately on data from a sample of users not representative of the global population, communities have expressed concerns on whether LLMs' outputs are sufficiently aligned with their values and may even be used to subvert them.

[2]Capgemini ([2024]). A time of transformation for the public sector: Using generative AI to move public services forward.
[3]Brunet, K. Et al. ([2024]). New defenses, new threats: What AI and Gen AI bring to cybersecurity. Capgemini Research Institute.

1.3 How will digital sovereignty help?

So, while the discussion around digital sovereignty is not particularly new, the rise of GenAI has increased the discourse's urgency. But what exactly does digital sovereignty mean? In essence, digital sovereignty refers to the independent control a state or entity exercises over its data, technology, and infrastructure. Although autonomy is at the core of digital sovereignty, the concept also includes resilience, strategic capability, and the ability to shape the rules and values that govern digital ecosystems.

Digital sovereignty originates in robust policy and regulatory frameworks, manifests in the availability of semiconductors and requires the nurturing of digital talent. While infrastructure, be it cloud capacities or support infrastructure providing access to energy and connectivity, is an integral part of digital sovereignty and takes a prominent place in discussions about the former, full digital sovereignty aims much larger. In short, it encompasses end-to-end control over the entire digital value chain.

Nonetheless, achieving full sovereignty across all stages of the value chain is typically neither feasible nor desirable. Instead, a globally integrated digital stack remains the most efficient and scalable approach for many use cases. To this end, the strategic focus should be on building a flexible and modular toolkit of sovereign technologies – particularly in areas where autonomy is critical. This includes scalable AI solutions that can be deployed when sovereignty requirements arise, ensuring that a state retains control over sensitive domains without isolating itself from global innovation.

"Digital sovereignty is neither a monolith in requirements nor in its solution. Instead, it's a broad set of categories with varying levels of magnitude."

Digital sovereignty is not a monolithic concept. Rather, it comprises multiple dimensions, each with varying relevance depending on the operational context, as depicted in Figure 1. These dimensions typically include:

- **Data sovereignty** – control over data storage, access, and governance, ensuring its localization, traceability and accessibility.
- **Operational sovereignty** – autonomy and resilience in managing and executing digital operations safely, often with the support of an ecosystem of sovereign partners.
- **Technical sovereignty** – ownership and control of technological infrastructure and capabilities, such as technologies' portability, reversibility and interoperability.

In addition to the above, the concept of **legal sovereignty** has recently come into the spotlight as a topic that has an influence on all three dimensions:

- **Legal sovereignty** – power of a state to establish and enforce the legal norms, regulations, and jurisdictional claims that govern digital infrastructures, technology actors, services, and data within its territory.

1.4 Why not all use cases require sovereignty

Additionally, digital sovereignty is not a binary condition that is either given or not. Instead, it can be thought of as a gradual concept, embracing each of its individual dimensions. This differentiation is essential to move current discussions beyond arguments on whether full digital sovereignty is or can be achieved.

Indeed, not all use cases in the public sector are critical for digital sovereignty and not all use cases that are pertinent to digital sovereignty require full control over the whole digital value chain. For example, in the context of public sector cloud infrastructure, achieving digital sovereignty requires that the service provider guarantees both legal and operational sovereignty, including protection against intercessions from extraterritorial jurisdictions. Additionally, ensuring data sovereignty is imperative to safeguard the integrity and confidentiality of the processed data. Safeguards embedded within contractual law and the extraterritorial applicability of data protection frameworks strengthen the security of data, even when a state has no technical sovereignty over the data.

Understanding how the interplay between the different dimensions (as well as the additional legal sovereignty aspect) determines the degree to which a country can achieve digital sovereignty. The ability to effectively navigate the trade-offs between dimensions is essential for policymakers, industry leaders, and technologists alike. Indeed, in an era defined by rapid technological advancement and geopolitical uncertainty, this concept has evolved from a theoretical aspiration into a practical necessity for many states – especially in Europe.

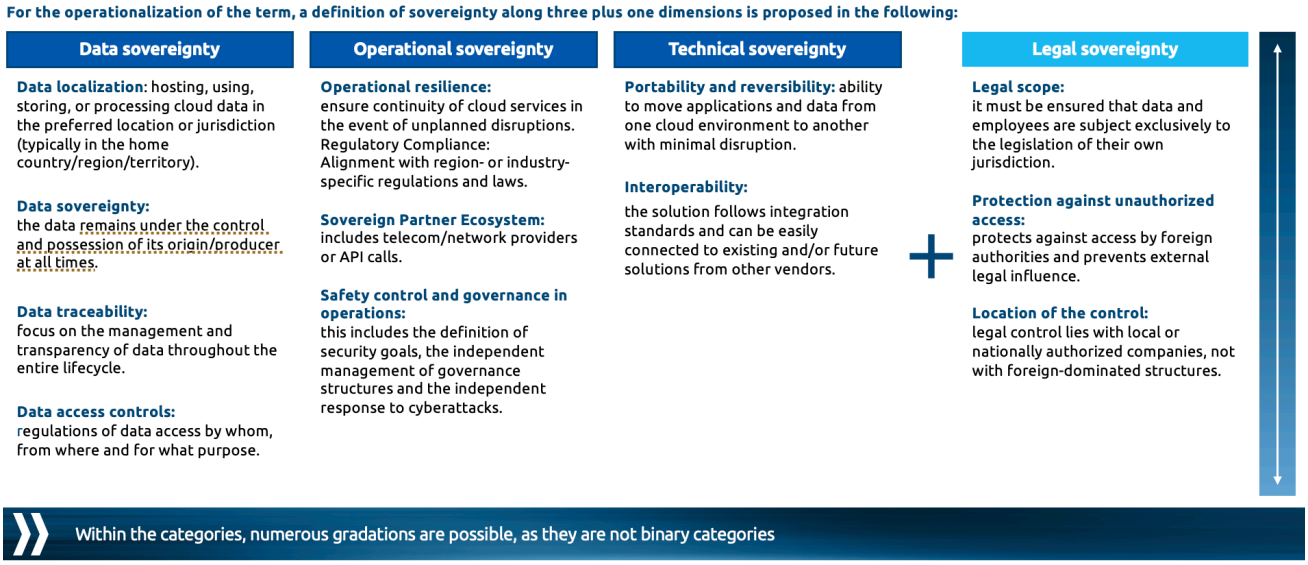


Figure 1: Overview of key dimensions of digital sovereignty

02

The importance of digital sovereignty for Europe in the age of GenAI

2.1 The digital sovereignty imperative in Europe

While digital sovereignty is an aspiration for many governments around the world, it is a strategic imperative in Europe for several reasons.

First and foremost, Europe is particularly exposed to the current geopolitical dynamics, as underlined by Russia's invasion of Ukraine and its repeated attempts to challenge Europe's post-Cold War security architecture. This situation is exacerbated by the ongoing geopolitical pivot of Europe's main ally, the United States, towards East Asia. Beyond direct challenges to the territorial sovereignty of European countries, attempts by actors interested in Europe's destabilization also include attacks against European countries' critical infrastructures and public administrations. As these threats increasingly rely on digital technologies, so must their deterrence and, if necessary, appropriate countermeasures.

Increasingly, these threats leverage GenAI, such as LAMEHUG, a malware attributed in July 2025 to a Russian government threat group that uses a large language model to automate system reconnaissance and data theft.[4] Similarly, GenAI is essential to the implementation of large-scale disinformation and manipulation campaigns aimed at undermining Europeans' trust in their governments and other public institutions. Without the capacity to develop and effectively deploy digital technologies on their own – i.e., without digital sovereignty – European democracies are vulnerable to the growing threats of antagonistic actors.

Second, Europe has emphasized its desire to ensure a responsible and human-centered digitalization that respects the European Union's (EU) fundamental values of human dignity, freedom, democracy, equality, rule of law and human rights. This desire is showcased through regulatory initiatives such as the EU General Data Protection Regulation (GDPR), the EU AI Act and the EU's Digital Markets Act.

These regulations also have important implications for the development and usage of GenAI technologies, which are governed by the EU AI Act's provisions on general-purpose AI. The risk classification of AI systems and their use cases as established by these provisions clearly reflects the EU's endeavor to embed its values in technologies through regulation. More generally, they highlight the EU's willingness to constrain the accumulation of economic power by technology conglomerates – especially by

[4]Hacioglu, S.O. (August 11th, 2025). LameHug: The First Publicly Documented Case of a Malware Integrating a LLM. Retrieved on September 28th, 2025, on Picus Security.

foreign ones. However, if few equivalent domestic technology alternatives are available, European initiatives to ensure that its values are embedded in foreign technology are unlikely to be effective.

Third, with government expenditures in the European Union amounting to, on average, ca. 49 % of GDP,[5] improving the efficiency and effectiveness of European public sectors through digital technology is essential to ameliorating Europe's quality of life. Generative AI offers enormous potential to modernize European public administrations and make them more responsive to the needs of European citizens. The possible applications are diverse and range from accelerating planning and approval procedures or automating both routine and complex tasks to improving the quality of administrative services for citizens. In the example of Germany's public sector, where a combination of increasing regulation and shrinking working-age population resulted in a large and growing shortage of 570,000 workers in 2024 (dbb, 2025),[6] harnessing the potential of GenAI is crucial. This includes, for example, the creation of standard documents such as notices or the answering of recurring requests. Effectively collaborating with AI, employees can then use the freed-up capacities for more demanding tasks that require human expertise or intensify personal exchange with citizens. Even for more complex tasks (e.g., application reviews, data-driven policing or citizen requests), generative AI tools can serve as valuable assistants to public servants and may improve interactions with citizens.

Beyond the potential of GenAI to improve European citizens' quality of life, such digital technologies are increasingly important for governments to meet citizens' expectations and, by extension, become essential to the preservation of social cohesion. But to fully exploit GenAI's potential in the public sector, it is essential to rely on sovereign AI solutions based on European values such as data protection, transparency and the rule of law.

2.2 Why more domestic technology solutions are needed

In stark contrast to the evident need of Europe's public sector for digital sovereignty stands its dependence on foreign technologies. For instance, the Draghi Report has highlighted that over 80% of the digital products, services, infrastructure and intellectual property are imported from abroad.[7]

Yet, the EU's efforts to achieve sovereignty by regulation will fall flat if there are no/ too few domestic technology solutions. This lack of home-grown solutions carries the risk that sensitive citizen and company data will fall into the wrong hands. In addition, geopolitical tensions can lead to bottlenecks in the supply of critical hardware and software components, which might jeopardize the effective functioning of the state and erode the trust of citizens. For example, the share of semiconductor manufacturing capacity headquartered in

[5] European Commission (2025). Government finance statistics: Government revenue and expenditure. Retrieved on September 25th, 2025.
[6] DBB (2025). Monitor öffentlicher Dienst. Berlin: DBB Verlag.
[7] Draghi, M. (2025). The future of European competitiveness. Part A | A competitiveness strategy for Europe. Luxembourg: Publications Office of the European Union; p. 56.
[8] European Commission (2022). A Chips Act for Europe. European Commission Staff Working Document (2022) 147.

Europe decreased from ca. 20 % in 2000 to about 9 % in 2020.[8] Regarding (Gen)AI, the dominance of non-European providers is also striking: Since 2017, 70% of the basic AI models have been developed in the USA and 15% in China (LEAM.AI, 2023).[9]

As European democracies navigate an increasingly complex global landscape, their current dependence on external digital infrastructures and technologies poses significant risks.

The urgency of strengthening European digital sovereignty is apparent in several European governments' endeavors to prioritize sovereign technology stacks to reduce external dependencies, including:

The Netherlands' parliament approved a number of motions calling on the government to reduce its reliance on U.S. software companies. Among the proposals was the development of a Dutch-controlled cloud services platform. As reported by Reuters, while such initiatives have previously faltered due to an absence of feasible European alternatives, lawmakers point to changing relations with the United States as a motivation giving the issue renewed urgency.[10]

The German government has taken a bold step forward by outlining a 4-year agenda focused on digital sovereignty, emphasizing support for European technology providers, securing national digital infrastructure, and laying the groundwork for a sovereign "Germany stack".[11]

Yet, though these national initiatives are important, taking a supranational approach towards digital sovereignty is crucial to safeguard Europe's security and capability to innovate. At the European level, this has been echoed by EuroStack, which warns that without decisive action, the foundations of European governance could be undermined.[12] In this context, the European Commission's launch of the AI Continent Action Plan, which aims to enhance Europe's AI capabilities through the mobilization of €200 billion for investment in AI via its InvestAI initiative, is a very positive signal.[13] As a testament to this momentum, European Commission President Ursula von der Leyen recently emphasized that a European AI is essential for our future independence in her State of the Union address.[14]

Together, these efforts highlight a decisive shift: Europe is not only recognizing the importance of digital sovereignty but is taking active steps to achieve it. But for these steps to yield a digital future in which Europe has sovereignty over its use of GenAI technologies in the public sector and beyond and can thus leverage them in line with its core values, a nuanced and strategic approach is key, as the next section explores.

[9]LEAM. AI. (2023). Large AI Models for Germany – Feasibility Study 2023.
[10]Sterling, T. (March 18th, 2025). Dutch parliament calls for end to dependence on US software companies. Retrieved on September 28th, 2025, on Reuters.
[11]BMI - Press - Germany launches government cloud
[12]EuroStack
[13]European Commission (2025). AI Continent Action Plan. Brussels: European Commission.
[14]State of the Union 2025 - European Commission

03

How Europe can achieve digital sovereignty in GenAI and beyond

Now, more than ever, with the advent of GenAI technologies, achieving digital sovereignty is critically important for Europe, but to do so effectively and efficiently, it must embrace an approach that is (i) pan-European, (ii) holistic, (iii) end-to-end, (iv) continuous and (v) multilateral. The result of such an approach is a sovereign AI technology stack that underwrites the independence and capability of Europe's public sector and embeds European values.

3.1 The need for a pan-European approach

The breadth and depth of the challenge of ensuring digital sovereignty is too large for any single European democracy to achieve on its own, thus a pan-European approach is needed. This perspective is prominent in the EuroStack initiative, a strategic program designed to integrate and develop both logical and physical digital infrastructures in Europe – an initiative to which Capgemini is a proud contributor.[15]

EuroStack promotes sustained investment in European digital public infrastructure, reducing reliance on non-European providers and ensuring that services for citizens, businesses, and institutions are secure, resilient, and aligned with European values. It also fosters innovation, enhances competitiveness, and supports the creation of governance frameworks that reflect Europe's democratic and legal principles.

While a pan-European approach to digital sovereignty doesn't exclude national initiatives with the same objective, such initiatives should be integrated to avoid a situation where every European country redundantly develops its own sovereign technology stack. Particularly in small European countries, a national approach is likely to result in thinly funded and incomplete technology stacks that fail to effectively foster digital sovereignty. Instead, under a supranational umbrella, European governments should strategically focus on developing certain capabilities while partnering with reliable European partners to cover capabilities that they don't have on their own.

The EuroStack Directory, which helps European public sectors procure digital products and services more efficiently by raising awareness for already existing European services and open-source technologies, is an example of how this approach can be put into practice – especially given that many IT leaders and procurement officers indicate being unaware of viable European alternatives.[16]

[15]Caffarra, C. et al. (2025). Deploying the EuroStack: What's Needed Now. Retrieved on September 28th, 2025, on EuroStack.
[16]Wire (August 12th, 2025). The State of Digital Sovereignty in Europe. Retrieved on September 28th, 2025, on Wire.

"The rise of GenAI has highlighted that digital sovereignty is not only covered by the location of a datacenter but for instance encompasses values as well. It can only be solved by looking at the whole TechStack."

3.2 Holistic thinking for Europe's digital sovereignty

In line with its pan-European perspective, digital sovereignty in Europe must be approached holistically, i.e., across its legal, data, operational and technical dimensions. Related to all other dimensions, Europe needs to affirm its control over the legal and regulatory frameworks pertinent to digital sovereignty. The necessity for legal sovereignty has become more apparent in recent years due to particular legislation and political influence concerning digital technologies and especially GenAI in geographies such as the United States and China.[17] In particular, European legal sovereignty in digital matters needs to be expanded and harmonized, asserted over cross-border data and services, duly reflected in public procurement and complemented with adequate enforcement capabilities.

In the realm of **data sovereignty** (one of the aforementioned digital sovereignty dimensions), Europe must ensure data – the fuel of modern AI – that is collected, stored or processed in Europe is also subject to European laws and governance structures. The EU's General Data Protection Regulation (GDPR) acts as a legal cornerstone of European data sovereignty by asserting jurisdiction over any entity processing EU citizens' data, independent of where the entity is located. Yet, data sovereignty not only relates to the way in which the personal data of EU citizens is handled but has also puts the composition

[17]Sayers, O. (May 23th, 2025). Microsoft's ICC email block reignites European data sovereignty concerns. Retrieved on September 28th, 2025, on ComputerWeekly.com

of training data into the spotlight. Here we see the EU AI Act acknowledging that governments and societies may have a legitimate interest in controlling the training data of AI models and systems if applied to politically sensitive cases. Such focus comes as no surprise in light of research by the Manhattan Institute, displayed in Figure 2, which shows that the political leaning of models' training data can strongly influence the outcome of their applications.[18]

Why is this a particular concern for Europe? Without sovereignty over the data upon which they are trained, AI systems in use in the EU may fall prey to biases unaligned with the heritage and vision of Europe – a risk accentuated by an increasingly unpredictable political climate and the interests of non-European technology conglomerates. For example, prominent U.S. technology firms have chosen to abstain from signing the EU's Code of Practice for General-Purpose AI, implying an unwillingness to offer more transparency on their training data.

A further integral part of data sovereignty is a large-scale sovereign data infrastructure based on European cloud providers and data centers that ensures sensitive data remains in Europe, is not exposed to access by foreign authorities, and allows European organizations to comply with GDPR without harm to their competitiveness. Initiatives such as GAIA-X, which was launched in 2020 to build a federated, secure and interoperable cloud infrastructure based on European values, are key to achieving data sovereignty in Europe. In addition, data sharing initiatives and dataspaces within Europe enable the pooling of data in a way that yields a strong training data foundation.

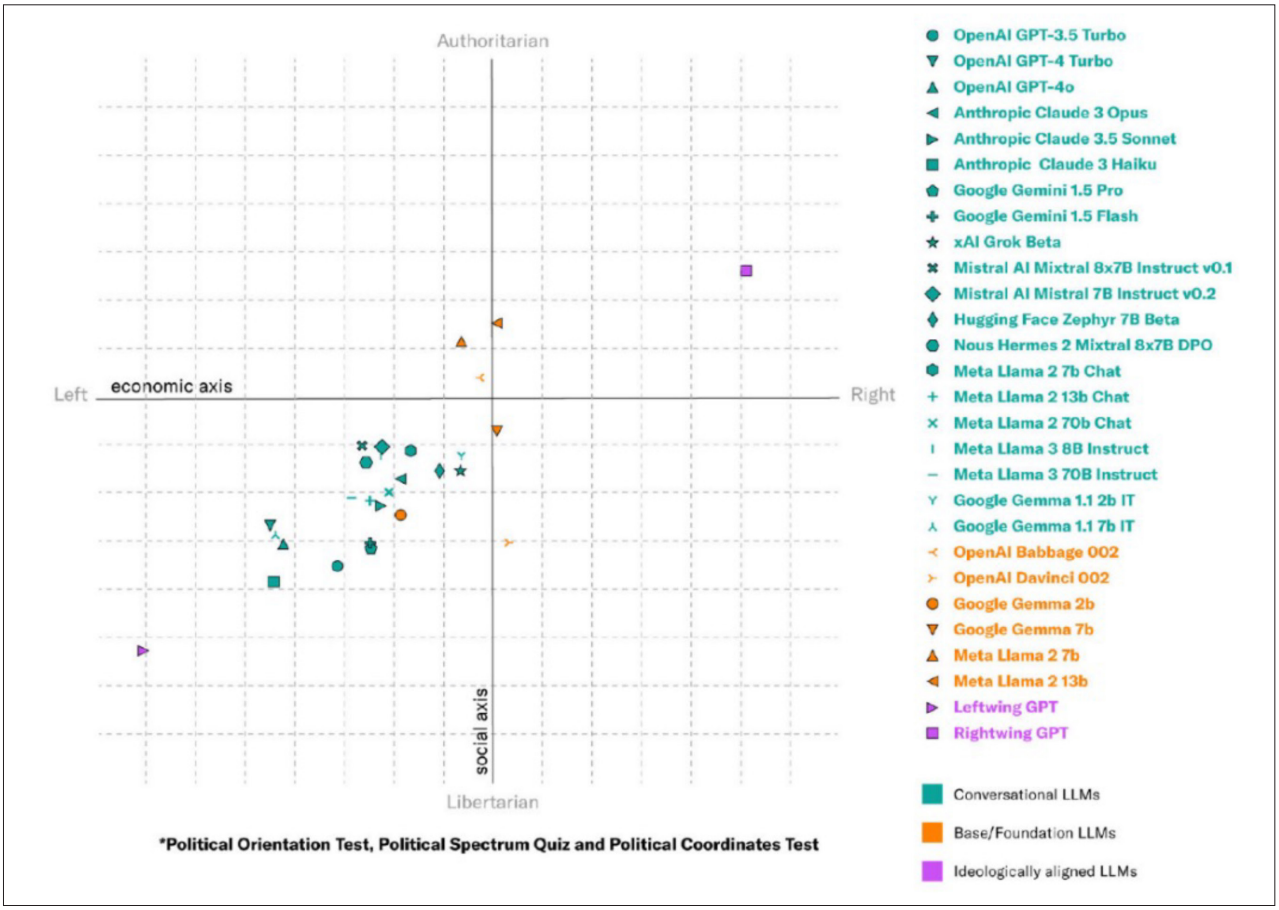


Figure 2: Average LLM Results Across 3 Political Orientation Tests. Source: Rozado (2025).

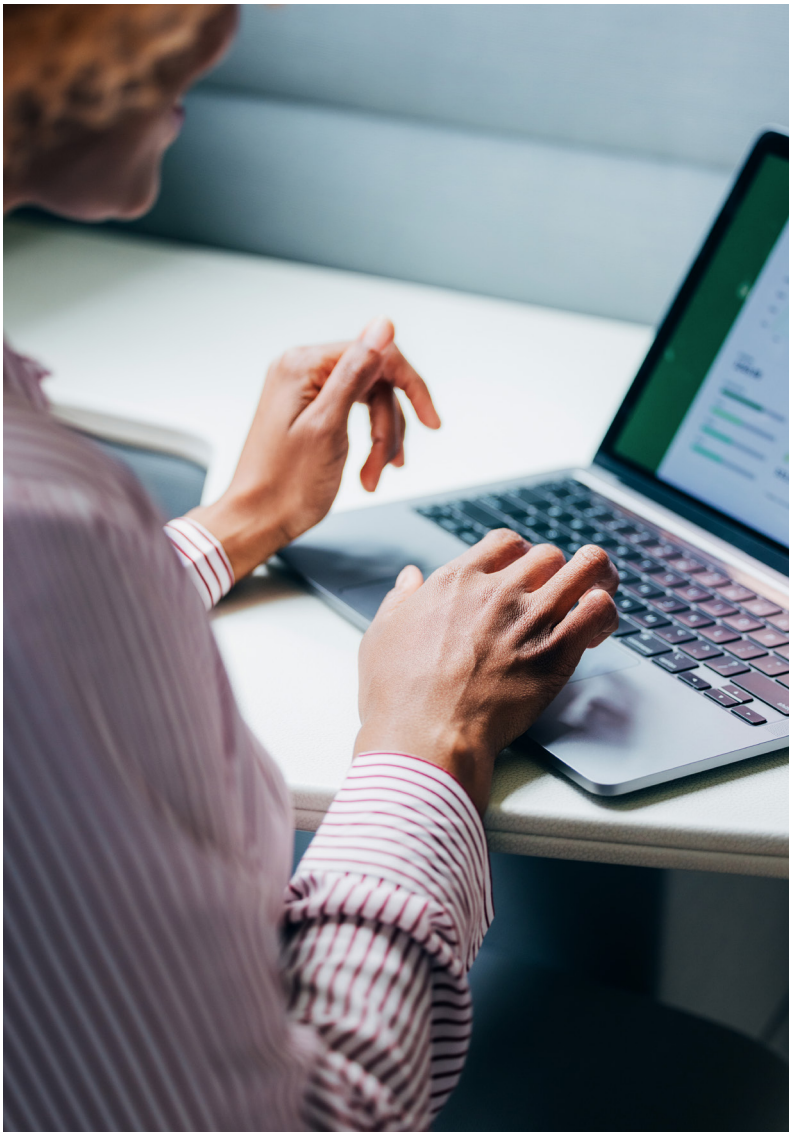
[18]*Rozado, D. ([2025]). Measuring political preferences in ai systems: an integrative approach. new york: manhattan institute*

The development of digital infrastructure – in particular the setup of EU-native cloud platforms and the strengthening of resilient, modular and interoperable digital public infrastructure – is also a key aspect in achieving **operational sovereignty** in Europe. However, unlike many sovereignty discussions limited to infrastructure would suggest, it goes beyond the infrastructure itself.

Operational sovereignty (the second of our sovereignty dimensions) includes the layer of human-AI chemistry where use cases are implemented, humans interact with AI and important ethical decisions are made in practice. As mandated by the EU AI Act through its AI literacy principle (EU AI Act, Art. 4), users of AI systems need to be well-equipped to interact with AI responsibly and designers of AI systems must ensure that this layer reflects European values if they are to be deployed in Europe. Besides this mediation layer, operational sovereignty also requires the establishment of structures and procedures that enable resilient, safe and controlled performance.

In turn, the **technical sovereignty** dimension focuses on the development and control of technology itself, including control over Europe's access to hardware such as microchips, servers and network infrastructure and software such as operating systems and enterprise applications, as well as the setting of technical standards and protocols. In the context of GenAI, an important building block of technical sovereignty are large language models. Open-source LLMs offer the advantage of being transparent and customizable, which allows for them to be tailored to the specific needs of public administrations. Moreover, adaptable models and reusable concepts are also important to increase the efficiency and scalability of AI solutions in public administration, as it allows to reduce development concepts and accelerate AI implementation.

Technical sovereignty also requires for European actors to be able to move data, applications or services between systems – portability – and to be able to terminate a service and retrieve all data and configurations in a usable format – reversibility –, for which the EU Data Act has created important provisions, including the transferability of digital assets and the elimination of switching charges.



3.3 Adopting an end-to-end approach

Any approach to European digital sovereignty must be conceived of as end-to-end, i.e., it must address all layers of the technology stack and cover the entire GenAI value chain, ranging from raw materials and energy over microchips, networks, cloud infrastructure, software and data.[19] However, to be truly empowered as an end-to-end stack, these layers must be integrated with each other. This perspective is emphasized by the EuroStack initiative, which identifies the bundling of European technology offerings and the assurance of their interoperability with hard- and software developed by mainly U.S. and Chinese players as key obstacles to these offerings' international competitiveness.

Importantly, addressing all stages of the GenAI value chain does not mean that Europe needs to develop competitive offerings for each stage's components. For instance, while U.S.-based NVIDIA is a global leader in graphical processing units (GPUs) and parallel computing software, both of which are essential to LLMs and therefore GenAI, the Dutch company ASML's strategic positioning as the world's only manufacturer of extreme ultraviolet lithography machines, which are the only equipment able to etch integrated circuits onto silicon with a nanometre precision, balances NVIDIA's impact on European digital sovereignty within the microchip layer.

[19] *Bria, F., Timmers, P., & Gernone, F. (2025). EuroStack – A European Alternative for Digital Sovereignty. Bertelsmann Stiftung.*

"Sovereignty cannot just be purchased or adopted when convenient. Governments and technology vendors need to work together. Either we succeed together or not at all."

3.4 Why continuous endeavor is paramount for sustained success

Sovereignty cannot just be purchased or adopted when convenient; instead, Europe's endeavor regarding its digital sovereignty must be continuous and sustained. Achieving a high degree of digital sovereignty in Europe is not something that can be achieved within a few years. Instead, it will require a long-term effort sustained over many years and – in certain domains possibly decades – to catch up with the technological state-of-the-art, so that a decision for European technology as rarely as possible implies a decision against excellent quality.

To sustain such an effort, it is essential that all stakeholders engaged in the pursuit of European digital sovereignty communicate consistently and repeatedly the reasons why such a pursuit is worthwhile and what Europe risks to lose if it fails to undertake it. Moreover, once Europe has achieved a high degree of digital sovereignty, it must not fall back into complacency and scale back initiatives aimed at that goal. Rather, Europe should create and expand structures that enable the ongoing governance, monitoring and adaptation of technologies, especially those pertinent to threats and geopolitical shifts – such as GenAI.

3.5 Collaboration is vital in a multilateral approach

Finally, as achieving digital sovereignty requires an integrated engagement regarding the development, acquisition and deployment of technology, a multilateral approach is key. The example of GenAI technologies, whose secure deployment in the public sector often requires a combination of substantial funding, advanced technical expertise, regulatory knowledge and trust, highlights the need for close collaboration between various stakeholders. Importantly, these stakeholders – especially the public sector participants – don't have to be at the national level; digital sovereignty is a matter that concerns not only governments but also regions, cities and even local institutions such as schools. To achieve digital sovereignty, stakeholders must set differences aside and jointly create the necessary momentum for transformation – with investments and contributions from all. The AI Factories at the heart of the EU's AI Continent Action Plan, which are partly funded by the EU but require the contributions of commercial actors, exemplify this perspective. If successful, they could constitute a major step not only towards improving Europe's digital independence but also towards catalyzing further public-private cooperation on AI more generally. Indeed, this notion of the private sector having a key role to play in achieving digital sovereignty in Europe is at the center of our call for action.

04

Towards a sovereign GenAI stack for Europe: a call to action

As set out in this paper, the application of GenAI in Europe's public sector holds enormous potential for accelerating cumbersome administrative processes, relieving overburdened public servants and – most importantly – improving the quality of public services for citizens. Against this background, a sovereign GenAI technology stack based on open standards and European values is the key to more digital sovereignty and parallels current public sector legislation and policy momentum. Such a stack stands at the center of a pan-European, holistic, end-to-end, continuous, and multilateral approach to strengthening Europe's digital sovereignty and overcoming its current dependence on U.S. and Chinese technology platforms.

4.1 Creating an overarching framework

Many of the building blocks for creating such a sovereign GenAI stack for Europe already exist and opportunities for their deployment in the public sector abound: From federated multi-cloud solutions for governments over trusted cloud architectures that ensure legal immunity from non-EU jurisdictions to sovereign off-site backups to protect public data in case of cyberattacks – technology must support secure, interoperable, and resilient public services in Europe. What is now needed is a collaborative effort to integrate them into a cohesive, overarching framework. Once such a framework is put in place, Europe will be well positioned to become a global leader in the large-scale and value-based adoption of AI in the public sector.

Far from a retreat into digital isolation, the creation of a European sovereign GenAI stack may serve as a springboard for cooperation with polities such as India or the African Union that also strive for digital sovereignty. For instance, in line with Europe's strategic interest to deepen its international partnerships and forge new ones, a sovereign GenAI stack based on open standards may also serve as a focal point for polities that share European values and induce them to integrate their technology offerings with the stack.

In such a context, Europe's emphasis on transparent, traceable and human-centered AI isn't a drawback but becomes a competitive advantage.

4.2 Alignment on GenAI across Europe

But while achievable, the development of a sovereign GenAI stack for Europe and its broad deployment in public administration is not a foregone conclusion and requires overcoming numerous challenges, from ensuring transparency and explainability to complying with complex legal frameworks. In the face of these challenges, this white paper aims to call to action a nucleus of European stakeholders that work together to both foster the development of those building blocks that are missing in the stack and to ensure their cohesive integration into an ecosystem of sovereign technologies.

Given that such an endeavor must be fundamentally multilateral, a broad coalition of stakeholders from politics, public administration, science and business must unite their efforts to help an AI-enabled public sector become reality, for example by:

- Creating the necessary framework conditions
- Investing in research and development
- Strengthening the AI competences of public servants.

In particular, greater alignment is needed between European governments and the technology, enabling the latter to act as strategic partners in developing modular offerings that can be easily integrated into an overall stack tailored to the needs of the public sector.

4.3 Witnessing steady progress in Europe

This call to action to create a sovereign GenAI stack for Europe is not speculative. Instead, Europe is already making tangible progress and is witnessing a surge of promising initiatives from its technology industry that are aimed at reinforcing digital independence in GenAI and beyond.

- In line with the above call to action, StackIt, Mistral, AlephAlpha, the Fraunhofer Society and Capgemini have joined forces to create a modular AI system that aims to rapidly accelerate German public administration's handling of very large numbers of complex planning and approval processes while maintaining full transparency and explainability along all steps.
- Similarly, TeleNor, NVIDIA and Capgemini are working together to build up a sovereign AI Factory in Norway.

Together, these examples highlight how courageous players can be at the vanguard of enhancing Europe's endeavor to be more resilient, future-ready and autonomous. What has made Europe strong throughout the past is the ability to look beyond differences and focus on what unites. In this spirit, let us now take bold action for Europe, in the words of the European Commission, "to become a global leader in the field of artificial intelligence, to become a leading AI continent".

[20] *European Commission ([2025]). AI Continent Action Plan. Brussels: European Commission.*

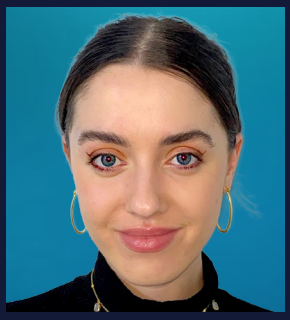
Authors

Oliver Stuke
Global GenAI Public Sector Lead
Capgemini Invent Germany

oliver.stuke@capgemini.com

Thordur Arnason
Global GenAI GTM Lead
Capgemini Invent Global / Norway

thordur.arnason@capgemini.com



Laura Laycock
Global GenAI Public Sector Ambassador
Capgemini Invent UK

laura.laycock@capgemini.com

Hector Niehues-Jeuffroy
Manager Data Driven Public
Capgemini Invent Germany

hector.niehues-jeuffroy@capgemini.com

Dr. Jakob Efe
Manager Data Driven Public
Capgemini Invent Germany

jakob.efe@capgemini.com

About Capgemini

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2024 global revenues of €22.1 billion.

www.capgemini.com