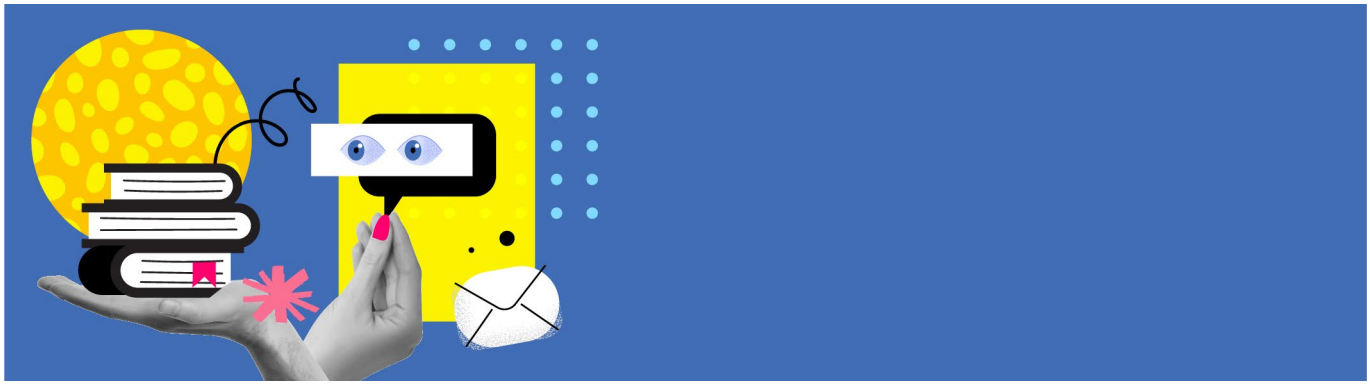
European Commission

Joint Research Centre

SCIENCE FOR POLICY BRIEF – Digital Public Governance



Strengthening Digital Sovereignty in EU Public Governance

A strategic imperative

2026

HIGHLIGHTS

- Europe is facing a tangible technological **'kill switch'**, that is, there is a fast-growing power imbalance centred on there being an uncontrolled technological dependency on a few gatekeepers in EU critical and strategic areas. This is especially the case in the public sector, where **70 % of public services are dependent on foreign-controlled data** and around 90 % rely on technologies and software from a single provider from outside the EU.
- With the public sector being responsible for governing strategic socioeconomic areas, while creating public value rather than profit, digital sovereignty involves more than a simple shift of power. It must be understood as the capacity to operationalise these values through **digital autonomy, allowing for some calculated and well-monitored digital dependencies** while actively managing them and without requiring complete isolation.
- Digital sovereignty is not an absolute condition, but rather a dynamic concept whereby different systems require distinct levels of priority, control, oversight and independence. The goal is not autarky or technological nationalism, but rather **optionality through open-source interoperable alternatives and agile alliance models**.
- EU Member States do not need to own everything; instead, they need meaningful freedom of action. Some Member States are paving the way to digital sovereignty by de-risking critical dependencies, while **building and progressively adopting alternative systems that are independent, interoperable, interchangeable, interconnected and collaborative**.
- Sovereignty in the EU public sector is not a single goal. Instead, it should be considered continuous active management and a balance of priorities driven by common values, thereby **reframing digital sovereignty from a question of ownership, control and compliance to a strategic imperative of responsibility and stewardship**, with public administrations leading by example.

Understanding digital sovereignty for public governance

Digital sovereignty has emerged as a central pillar of European strategic autonomy – as outlined in the recent EU communication on technological sovereignty – through two legislative proposals and four key initiatives. In particular, the Cloud and AI Development Act and the open-source strategy both require a rapid shift of the EU's position from a having a reactive focus on resilience and risk mitigation to taking a proactive approach that is grounded in technological sovereignty.

In a recent JRC *Science for Policy* brief[1], digital sovereignty is described as the capacity to hold strategic independence in the digital domain while remaining open to global collaboration and aligning with democratic values. Digital sovereignty requires capacity not only in data governance but also and especially across the entire digital value chain, or stack, including secure and resilient infrastructures, technological development, standards setting and strategic supply chains.

Public sector organisations play a key role in this landscape as they are both the main procurers and the main users of digital technologies. In this scenario, the present *Science for Policy* brief unpacks the many components of **digital sovereignty specifically through a public sector and public governance lens**. In doing so, the brief explores what digital sovereignty involves for the public sector, outlines the current status of EU dependency on foreign big tech companies, provides an analysis of risks and opportunities and – while drawing attention to the socioeconomic importance and implications of digital technologies in enabling public governance and public services delivery – delivers a number of recommendations in strategic areas of interventions. The more specific context and implications for public administrations are discussed in a separate publication[2].

Unlike private sector organisations, which are driven by profit maximisation, organisations in the public sector aim to deliver value creation for the common good, operating within highly diversified and complex political, cultural and socioeconomic ecosystems. Public sector organisations are responsible for governing strategic socioeconomic areas, including health, social security, migration, defence, energy, the environment, justice and education, which in turn become critical priorities and infrastructures in line with geopolitical contexts and socioeconomic trends.

The current EU landscape: digital dependencies and the 'kill switch'

The reality of Europe's digital dependency on foreign actors and markets is stark when one looks at the hard figures.

The kill switch: hard figures

- Over 80 % of Europe's digital nfrastructure and technologies are not European, with 70 % of foundational AI models developed in the United States (US)[3].
- Over 70 % of the European cloud market is controlled by three US-based hyperscalers, while European providers hold only 15 %[4].
- In the public sector specifically, with govtech accounting for 14 % of EU gross domestic product[5], 90 % of public services rely on Microsoft technologies and software[6], with 70 % dependent on foreign-controlled data[7].

This dependency creates significant jurisdictional and operational risks for public sector organisations, particularly given the emerging geopolitical challenges, cybersecurity vulnerabilities and the fact that **the infrastructure and its governance costs are local, while the value extraction is global**.

> Many countries are gradually becoming consumers of infrastructure that they do not control, when financing grid upgrades, energy infrastructure and data centre expansion. Meanwhile, the long-term recurring revenues generated by those systems flow abroad and reinforce foreign incumbent ecosystems.

In this arena, fundamental questions emerge.

- **How can we effectively regulate, implement and manage policies in support of shared values and domestic interests when we do not own or control the underlying technologies and systems?**
- **How can we ensure that the assets created in Europe and their socioeconomic value benefit Europe?**

A concrete kill-switch case

Nowadays, more than 61 % of card transactions in the euro area are handled by US card brands[8] (with Visa and Mastercard having a combined share of the card payment value of 47 %[9]), while transactions in 13 of the 21 euro-area countries run exclusively on international card schemes. What would happen if such foreign incumbents decided to suspend these services as retaliation and a form of political pressure?

Challenges and opportunities

Europe is facing a power imbalance. With an uncontrolled technological dependency on a few gatekeepers in critical and strategic areas for the EU, there is a need to reshape digital sovereignty in the public sector, emphasising independent agency and choice in decision-making. This endeavour involves both opportunities and challenges, especially in strategic socioeconomic sectors. Table 1 outlines the strengths and weaknesses in the current technological and regulatory EU setting.

Table 1. Analysis of strengths, weaknesses, opportunities and threats: digital sovereignty in the EU public sector

Strengths	Weaknesses
Robust regulatory framework: regulations such as the General Data Protection Regulation, the Data Act and the AI Act provide a world-leading legal 'shield' and set out EU-based values.	**High vendor lock-in:** there is deep integration of foreign software within public sector workflows (e.g. Microsoft Outlook and Teams).
Open-source leadership: there is strong political backing for open-source solutions.	**Infrastructure gap:** there is a lack of local hyperscale capacity.
Values-based innovation: there is a focus on privacy and human-centric services (including the use of AI).	**Fragmentation:** there are 27 national procurement systems, diverse cultures and diverse languages.
Opportunities	**Threats**
The European tech sovereignty package (2026) provides a comprehensive strategy to support technological sovereignty.	**Brain drain:** talent is moving to higher-paying tech giants outside the EU.
Public procurement power: 'European preference' rules can be used to favour local small and medium-sized enterprises.	**Retaliatory protectionism:** trade countermeasures can be implemented against EU technology laws.

Source: Authors

From sovereignty to autonomy

Current conceptions of digital sovereignty often refer to a state's or entity's power to govern, control and protect its digital assets (data, infrastructure and technology) in accordance with its own laws, focusing on independence and reducing reliance on foreign technology. In this context, we highlight the importance of digital autonomy, that is, the practical capacity and agency to govern one's own digital data and systems independently and to shape outcomes within a broader, interdependent digital world, focusing on strategic control over technology choices, without requiring complete isolation.

To maintain the necessary continuity and efficiency in public governance, therefore, the goal is not necessarily complete independence, but rather '**intelligent dependence**' or '**strategic digital autonomy**', also referred to as **'managed independence'**[12]. This is a pragmatic approach that allows for some digital dependencies while actively managing them.

This means building domestic strengths and capacities, while using interdependence as a source of advantage and maintaining the agency to steer outcomes, protect national interests and capture and protect value(s) in a globally connected digital ecosystem.

It marks a shift away from a static idea of sovereignty towards a dynamic concept of agency, where sovereignty is not a single goal but a dynamic balance of priorities. It means de-risking critical dependencies while building alternative systems that are interoperable, resilient and collaborative.

Digital sovereignty therefore cannot be reduced to a single dimension or seen as an absolute condition. It exists in degrees and varies by context. Different systems may require distinct levels of control, oversight and independence.

Digital sovereignty implications for critical domains of the public sector

In the last few years, the EU has established a robust policy framework for supporting digital sovereignty across multiple domains.
Key regulatory and policy instruments include those directly relevant for the public sector, as set out in Table 2.

Table 2. Mapping critical public sector domains to regulatory foundations and strategic initiatives

Public sector domain	Key EU policy frameworks	Sovereignty implications and notes
1. Democratic infrastructure and governance	eIDAS 2.0 (2024), Interoperable Europe Act (2024), AI Act (2024), NIS2 Directive (2023), communication on European tech sovereignty package (2026)	Sovereignty as regards the infrastructure of democratic governance is a concern.
2. Public safety and security	NIS2 Directive (2023), Cyber Resilience Act (2024), AI Act (2024), ENISA cybersecurity certification framework (2019), Infrastructure for Resilience, Interconnectivity and Security by Satellite 2 network (2029)	Security by design for connected public safety infrastructure is a direct sovereignty concern.
3. Critical infrastructure management	Critical Entities Resilience Directive (2023), NIS2 Directive (2023), European Chips Act (2023), Data Act (2024), Digital Networks Act (Commission proposal 2026), communication on European tech sovereignty package (2026), Cloud and AI Development Act (2026)	The resilience of energy, transport, water and digital infrastructure should be considered, along with semiconductor supply chain sovereignty. In addition, open, interoperable and resilient digital ecosystems are required.
4. Healthcare and social protection	European Health Data Space Regulation (2025), AI Act (2024), GDPR (2016), Digital Governance Act (2023), NIS2 Directive (2023), *ENISA Threat Landscape: Health sector* (2023)	Foreign state actors targeting health infrastructure as part of hybrid warfare strategies bear sovereignty risks.
5. Education and research	European Research Area policy agenda (2025), Digital Governance Act (2023), AI Act (2024), digital education action plan (2021)	AI in education is classified as high risk; open science and the reuse of research data should be considered.
6. Justice and legal systems	AI Act (2024), Law Enforcement Directive (2016), e-Evidence Regulation (2023), eIDAS 2.0, Interoperable Europe Act (2024)	Some of the most tightly regulated high-risk use cases in the AI Act are in this domain.
7. Economic regulation and public procurement	Digital Markets Act (2023), Foreign Subsidies Regulation (2023), AI Act (2024), public procurement directives (under review), EU cloud sovereignty framework (2025), European open-source digital ecosystem strategy (2026), Cloud and AI Development Act (2026)	Procuring public authorities are also AI Act deployers with strict compliance obligations, in this case reducing platforms' dependency on foreign data and platforms.
8. Data governance and public registries	Digital Governance Act (2023), Data Act (2024), data Union strategy (2025), GDPR (2016), Interoperable Europe Act (2024), EU cloud sovereignty framework (2025), EU cloud rulebook (under review), Cloud and AI Development Act (2026)	The reuse of public sector data and limits on non-EU government access to EU data should be considered.
9. Public communication and information integrity	Digital Services Act (2023), European Media Freedom Act (2024), *Code of Conduct on Disinformation* (2025), European democracy shield and the related action plan (by 2027)	Sovereignty over the epistemic conditions of democratic governance should be considered, whereby citizens have agency to form independent political opinions.
10. International relations and diplomacy	EU–US data privacy framework (2023), Data Act (2024), 2030 EU digital compass, *G7 Hiroshima Process on Generative Artificial Intelligence (AI)* (2023)	The EU is a global AI norm-setter, as adequacy decisions remain legally fragile.

NB: eIDAS, Regulation on Electronic Identification, Authentication and Trust Services; ENISA, European Union Agency for Cybersecurity; GDPR, General Data Protection Regulation; NIS, Network and Information Security.

Source: Authors

Strengthening digital sovereignty for autonomous public governance

To be able to address diverse needs and objectives, effective public governance needs to be operationalised at **multiple organisational levels** and in multidimensional environments and socioeconomic ecosystems. This needs to take place through heterogeneous governance models and requires specific organisational and collaborative strategies, diversified alliances and shared approaches, and digital technologies and infrastructures that are **independent, interoperable, interchangeable and interconnected**.

We can call this approach **the 'four Is paradigm'**.

The four Is paradigm provides a vocabulary to articulate how systems could work and relate to one another, from full autonomy to full integration, with interoperability and interchangeability as the thoughtful middle ground.

> The **' four Is paradigm'** refers to autonomous, integrated and sovereign EU digital systems solutions that are **independent, interoperable, interchangeable and interconnected**.

This shift would need to be done by considering a multilayered public governance environment, built upon **six operational levels**, each ruled by different yet interconnected regulations and administrative and legal frameworks, namely the **cross-border, national, regional, local, distributed and cross-sectoral levels**.

Digital sovereignty as stewardship of public values

EU public values such as transparency, accountability, equity, participation and respect for human rights are enshrined in EU digital regulations. Digital sovereignty in the public sector context must be understood as the capacity to operationalise these values by building upon the key pillars of the digital sovereignty framework[1], namely (1) people, (2) products and markets, (3) infrastructures and (4) governance. These pillars are based on the principles of digital autonomy and optionality.

This reframes sovereignty from a question of ownership, control and compliance to one of **stewardship**, agency, responsibility and accountability, in a globally interconnected system.

This involves **epistemic sovereignty** (the right to define knowledge systems in accordance with local contexts and values), **moral sovereignty** (the capacity to embed ethical principles into technological design) and **democratic agency** (ensuring that citizen-facing services support long-term adaptability and civic participation).

> Digital sovereignty in the public sector becomes not just a technical state but a **dynamic strategic orientation that balances multiple imperatives** simultaneously in diverse socioeconomic, technical, cultural and political contexts.

Strategic principles underpinning sustainable digital sovereignty in the public sector

Digital sovereignty in the EU public sector involves different extents of autonomy and managing interdependency in different sectors and actors, with assets, alternative solutions and strategies needing to be carefully coordinated. Achieving this requires moving beyond ideological debates and apply an approach built on key **strategic principles**.

Strategic principles of digital sovereignty

1. **Shared sovereignty and subsidiarity:** sovereignty is distributed across the national, regional and local levels, requiring coordinated governance mechanisms that respect subsidiarity while enabling interoperability, reusability and interconnection.
2. **Contextual and sectoral calibration:** different sectors (e.g. health, defence, energy and justice) may require varying levels of control and sovereignty.
3. **Resilient interdependence** rather than isolation: systems need to be built that are interoperable, resilient and collaborative, while de-risking critical dependencies by relying on alternative domestic technologies.
4. **People-centred outcomes:** it needs to be ensured that digital sovereignty translates into tangible benefits and agency for citizens.

5. **Responsible sovereignty:** the approach needs to be 'capable of responding' through careful listening, observation and understanding of actual needs, diverse contexts and specific goals, including preserving our environment and considering nature a rightful and legitimate partner

Digital sovereignty examples by public administrations in the EU

The use of digital technology by the public sector is critical not only for addressing priority assets, but also for society's most critical segments and vulnerable populations, for which it is important to preserve fundamental rights and create public value, rather than profit. While the context of and implications for public administrations are discussed separately[2], the following examples give a sense of direction.

Examples of digital sovereignty by public administrations in the EU

- Germany: in Schleswig-Holstein, 30 000 employee workstations were transitioned to open-source solutions, moving towards digitally sovereign IT workplaces, including digital sovereignty funds supporting open-source and independent standards.
- France: the sovereign open-source video conferencing platform Visio was used to phase out US-based collaboration platforms. France also launched its Digital Sovereignty Observatory to monitor and assess digital sovereignty and is piloting a Digital Resilience Index.
- Italy: the Ministry of Defence completed one of Europe's largest open-source migrations, transitioning 150 000 personal computers to LibreOffice; Italian procurement law now requires public administrations to consider reused or free software before proprietary licences.
- Spain: Barcelona invested heavily in open-source software as part of a broader digital strategy. The Government of Extremadura confirmed that thousands of healthcare-system personal computers run open-source office applications.
- The Netherlands: Amsterdam's digital autonomy plan was developed to address dependencies and establish pathways for municipal digital sovereignty.

Key pathways and recommendations

Digital sovereignty is not an absolute condition and, to be useful and sustainable, **it needs to be addressed in a hybrid and adaptative fashion** through strategic alliances, shared infrastructure, modular architecture and interoperable, open-source and reusable components.

In the given EU context, the aim should be to take a pragmatic approach to implementing **open, strategic digital autonomy** by focusing on operational freedom, **allowing for dependencies – managing rather than eliminating them** – and building sustainable collaborations.

To **reduce public governance ecosystem dependencies**, the following suggestions, stemming from the literature, public consultations and research results over the past few years, provide examples of possible actions within key areas of intervention and at different operational and governance levels. These would still need to be adapted and prioritised in line with specific contexts and needs to support the different foundations of multilayered digital ecosystems.

1. Infrastructure and technical capacity

- Invest in EU-made digital public infrastructure, scale up European digital commons and develop public computation infrastructure.
- Support framework conditions, for example by developing EU certification frameworks and trusted catalogues of open-source solutions.

2. Procurement and market shaping

- Reform public procurement processes and tools, guided by the principle of 'public money, public code', prioritising open-source and interoperable solutions.
- Prohibit vendors' lock-in technologies and make interoperability mandatory in public procurement specifications.
- Favour European open-source contributors and providers while prioritising non-price criteria in public procurement specifications.
- Leverage small and medium-sized enterprises and start-ups as instrumental assets for disruptive innovation and support their innovative govtech and civic-tech ecosystems.

- Develop alternative economic models for a 'fair' market, as opposed to a 'free' market (e.g. through the stewardship model).

3. Governance and standards

- Implement the 'four Is paradigm' across digital infrastructure layers.
- Establish coordinated EU governance, for example through the European Digital Infrastructure Consortium and dedicated funding schemes.
- Develop shared metrics and structured assessment frameworks, for example by mapping digital dependency indices to digital performance to derive digital sovereignty.

4. Skills and institutional capacity

- Reconcile the need for open, interoperable and sustainable public service solutions with the actual contextual needs defined by territorial conditions.
- Build comprehensive skill development in the public sector at all administrative levels.
- Foster new ecosystems and cooperation between the public and private sectors, non-profit actors and research institutions.

5. Data and artificial intelligence governance

- Establish common EU public sector data spaces, especially for strategic sectors.
- Advance public-interest AI principles based on EU values, open models, rights protection, co-design and responsible procurement.
- Recognise national data assets as reflections of a nation's reality and diversity, with provenance, inclusivity, privacy, security and stewardship as core principles.

6. Environmental sustainability

- Standardise life-cycle analysis methodologies for AI models and digital infrastructure.
- Require transparency from cloud service providers regarding environmental impact and energy efficiency.
- Prioritise energy-efficient computing infrastructure in public procurement decisions.

7. Operational avenues and exit strategies

- Conduct 'digital dependency risk assessments' for critical infrastructure systems and sectors.
- Develop mandatory exit and migration plans for high-risk foreign-controlled solutions and systems.
- Set clear requirements for EU-based source code access safeguards, open standards and data portability.
- Develop an EU-wide digital sovereignty risk register dedicated to the public sector.

Conclusions and prerequisites for progress

The EU already possesses the necessary ingredients for a public-value approach to digital sovereignty and public governance autonomy: comprehensive programmes and regulations, innovative industries, diverse talent, robust values, and strategic funding mechanisms. While the production and prioritisation of European solutions could be supported by enabling regulations and public procurement rules, key stakeholders in the emerging govtech ecosystem, networks of intermediaries, innovation investors and civil-society organisations offer collaborative capacity.

However, possessing some ingredients is not enough to address the underlying challenges. Assets, alternative solutions and pragmatic approaches must be coordinated, building on strategic alliances within a coherent project and driven by a common purpose.

Preconditions for success

- Provide alternative technologies and solutions based on open source, interoperable, and replicable technologies and infrastructure, built on domestic strategic components and assets.
- Deliver synergies across operational, governance and infrastructure layers to support dynamic distributed ecosystems and supply chains for sustainable digital public infrastructure and their enablers.
- Focus resources on the critical and strategic sectors in which public governance and its services are likely to have the greatest socioeconomic impact.
- Explore alternative economic models for easier access to domestic markets.
- Reconcile power imbalances through strategic partnerships and collaboration rather than competition.
- Match harmonisation requirements with contextualisation needs across different European territories, multilayered governance models, legal and operational diversities, and public, private and social actors.

Digital sovereignty in EU public governance involves much more than a simple shift of power. **It requires public sector organisations to lead by example through the progressive adoption of alternatives and the active management of critical dependencies, while ensuring that the necessary autonomy and capacity serve the public good.**

While the strategic push for digital sovereignty in the public sector is clear, untangling the existing interdependent digital ecosystems will require years of sustained investment, careful migration planning, institutional adaptation and political will. The goal is not autarky or technological nationalism, but rather optionality through open-source standards, interoperability, strategic resilience, strategic procurement and common infrastructure leverage.

The journey has begun, as demonstrated by current initiatives across Member States. Success will depend on treating digital sovereignty not as a destination but as a deliberate and continuous process of assessment, decision-making and adaptation to ensure that EU public digital infrastructure ecosystems and their governance genuinely serve public purpose and EU values.

Areas for future research

Based on the above, we identify three key areas for future research in this domain:

- developing digital sovereignty assessment frameworks and indices that are specific to the public sector and that combine digital dependency metrics with indicators of digital performance and public value;
- collecting and organising the existing evidence for assessments of the success of different policy approaches (procurement reform, open-source mandates and public computation investment) in achieving digital sovereignty in the EU public sector;
- Exploring alternative economic models to be used for a 'fair' as opposed to a 'free' market.

References

1. Di Marco, D., Thabit, S., Kotsev, A., Christensen, A., Minghini, M. et al., 'Open but not powerless: Towards a common understanding of EU digital sovereignty', *Science for Policy Briefs*, European Commission, Ispra, 2025, JRC144908.
2. Bryson, J., Danneels, L., Di Marco, D., Dobbe, R., Grimmelikhuijsen, S. et al., 'Advancing EU digital sovereignty in public administrations – Navigating opportunities, trade-offs and open questions', *Science for Policy Briefs*, European Commission, Ispra, 2026, JRC146997.
3. Bria, F., Timmers, P. and Gernone, F., *EuroStack – A European alternative for digital sovereignty*, Bertelsmann Stiftung, Gütersloh, 2025.
4. Telecom Review Europe, 'From code to strategy: The stakes of cloud dependency', 3 March 2026.
5. Niehaves, B. and Klassen, G., *Govtech Practices by Public Administrations – Influencing factors and recommendations to foster cross-border, interoperable public services in Europe*, Publications Office of the European Union, Luxembourg, 2026, JRC145627.
6. Prasad, K., Fazal, A., Nimbalkar, K. and Amin, A., *Quantifying EU Public Sector Dependence on Productivity Software*, Open Cloud Coalition, Brussels, 2025.
7. Gineikyte-Kanclere, V., Eggert, M. and Skiotyte, G., 'At a glance: European software and cyber dependencies', European Parliament, Brussels, 2025.
8. European Central Bank, *Report on Card Schemes and Processors*, Frankfurt am Main, 2025.
9. Szalay, B., 'Is Europe ready to reduce its reliance on Visa and Mastercard?', Electronic Payments International, 24 February 2026.
10. European Commission, 'Communication on European tech sovereignty, accompanied by an EU open source strategy', 3 June 2026.

The opinions expressed are those of the author(s) only and should not be considered representative of the European Commission's official position.

We extend our gratitude to Sven Schade and Luca Tangi of JRC Unit T1 and Mario Scharfbillig of JRC Unit S2, who have improved the quality and effectiveness of this policy brief.

How to cite this report: Manzoni, M., Farrel, E., Hernandez, L., Martin Bosch, J., Combetto, M., et al., 'Strengthening digital sovereignty in EU public governance: A strategic imperative', *Science for Policy Briefs*, European Commission, Ispra, 2026, JRC147599.

Science for policy

Scan the QR code to visit:

Joint Research Centre
https://joint-research-centre.ec.europa.eu

Contact information

European Commission, Joint Research Centre (JRC)
Contact: Marina Manzoni
Email: jrc-digital-governance@ec.europa.eu

© European Union, 2026
Reuse of this document is allowed, provided appropriate credit is given and any changes are indicated (Creative Commons Attribution 4.0 International license). For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders. All images © European Union, unless otherwise stated

JRC147599