

A woman with blonde hair, wearing a black coat and a blue scarf, is walking from left to right in the foreground. She is holding a blue folder or bag. In the background, there is a classical building with large white columns and windows with yellow curtains. The scene is brightly lit, suggesting daytime.

Digital sovereignty in the public sector Keeping the nation running

How to create a digital sovereignty
strategy to maintain independent
control and resilient operations ■



Digital sovereignty is vital to protect national interests and preserve citizen trust

In a volatile geopolitical landscape, and with new cyber threats emerging daily, governments and public sector organizations are recognizing the urgent need to regain control of the digital infrastructure, data, and technologies they rely on.

65% of public sector organizations say that achieving digital sovereignty is a strategic priority, with the sovereignty of data (77%), cybersecurity (72%), cloud (68%) and AI (61%) their greatest concerns.¹ But for many, the issue is hard enough to define, let alone resolve. Digital sovereignty is complex; it goes far beyond individual technologies to encompass a whole ecosystem of capabilities, standards, and governance models. It's a continuous evolution, not a one-off project.

To maintain operational resilience, strategic autonomy, and the integrity of citizen data and services, public sector organizations must establish the right levels of sovereign control and vendor assurance across the digital value chain.

In this guide, you'll discover:



What digital sovereignty means for public sector organizations



A structured approach for assessing your digital sovereignty posture



Practical applications of digital sovereignty in three public sector scenarios



1. Capgemini Research Institute, Data and AI in government 2026, www.capgemini.com/insights/research-library/data-and-ai-for-public-services



Defining digital sovereignty for the public sector

The EU Cloud Sovereignty Framework, which includes the banding of cloud services into Sovereignty Effectiveness Assurance Levels (SEAL), has brought the issue of digital sovereignty to the forefront of policymaking across member states and beyond.² This shift in thinking can also be seen in the EU's Cloud and AI Development Act (CADA), which explicitly links digital sovereignty to the need for governments to have strategic autonomy.³

Every public sector organization depends on an array of digital services to support day-to-day operations. To sustain business continuity, operational resilience, and strategic autonomy, organizations must control the data, software, algorithms, and infrastructure that power these services.

By defining and executing a comprehensive digital sovereignty strategy, public sector organizations can maintain control and assurance while accelerating the delivery of citizen services.



What is digital sovereignty?

Digital sovereignty is an organization's ability to maintain operational resilience and strategic autonomy while minimizing external interference across the digital value chain.

Assessing sovereignty across the digital value chain

While cloud sovereignty is a cornerstone of EU policy, it's just one piece of the puzzle. To build an effective sovereignty strategy, organizations must consider risk across the entire digital value chain and build sovereign capabilities in eight interconnected dimensions:

- **Cybersecurity:** The ability to prevent, detect, respond, and recover independently of foreign actors
- **Software:** Application portability and auditability, and freedom from vendor lock-in
- **AI:** Control over models, training data, and inference
- **Data:** Assurance of who can access, process, share, or compel disclosure of data
- **Cloud:** Oversight of who runs the infrastructure for cloud workloads
- **Connectivity:** Domestic legal and operational control of network infrastructure
- **Hardware:** Supply chain resilience for hardware components
- **Energy:** A resilient and controlled energy supply for digital services

2. European Commission, Cloud Sovereignty Framework Version 1.2.1, October 2025, [09579818-64a6-4dd5-9577-446ab6219113_en](#)

3. European Commission, Proposal for the Cloud and AI Development Act (CADA), June 2026: [proposal-cloud-and-ai-development-act-cada](#)



Four strategic perspectives for determining sovereignty risk exposure

To establish an appropriate digital sovereignty posture, it's essential to have a holistic view of sovereignty risk and take a structured approach to defining your strategy. By assessing your current sovereignty posture through four lenses, you'll build a complete picture of where your organization's key risks lie – and how to mitigate them:

1) Data and AI

- Assess whether essential data activities, such as collection, storage, analysis, and sharing, are conducted under strict national controls that align with government protocols and security classifications.
- Identify whether AI models are domestically sourced and trained on trusted, traceable datasets within sovereign infrastructure.
- Determine where data resides and whether you have control over its encryption – at rest, in transit, and in use.
- Establish who has access to data, at what level, and under what conditions.

2) Technology

- Identify whether you can assure uninterrupted access to digital services during normal operations and under exceptional circumstances.
- Evaluate your level of dependency on foreign suppliers across your hardware and software supply chains.
- Determine whether you can sever external access or quickly exit cloud services without penalty or loss of control over your data.
- Assess whether the architectures of your digital services are aligned with relevant security standards.

3) Operations

- Identify who has admin access – on consumer and provider sides – to your digital services and the technology that delivers them.
- Evaluate how individuals with access are vetted and trained, and whether they have appropriate security clearances, nationalities, and skills.
- Appraise your ability to ensure digital service continuity in day-to-day operations and maintain resilience during future disruptions.
- Establish the extent to which your infrastructure operations rely on foreign energy sources.

4) Legal and jurisdiction

- Identify the conditions under which foreign entities can compel data disclosure or instigate service and supply chain disruption and degradation.
- Evaluate your providers' transparency over legal ownership of design, manufacture, and operation.
- Assess whether you have legal ownership of your digital services.
- Determine whether all parties in your supply chain meet external compliance and certification mandates.



Finding the right sovereignty balance

Not every digital workload requires the same level of sovereignty. Your approach to closing the digital sovereignty gap will vary depending on the risk attached. For example, lacking sovereignty over a parking app might be an acceptable risk, but lacking sovereignty over air traffic control systems could be extremely dangerous.

That's why it's essential to start with a thorough assessment of the true sovereignty risks across your digital value chain.



Digital sovereignty in action: three public sector scenarios

To demonstrate how a digital sovereignty strategy can be applied in the real world, here are three public sector scenarios, ranging from an AI tool for a single organization to a complex data-sharing platform spanning agencies in multiple countries.

1. Deploying a cloud-based AI assistant to accelerate citizen service delivery

The scenario

In this scenario, based on a real Capgemini engagement in the German public sector, a large organization creates a chatbot to help thousands of employees work more efficiently.

This involves allowing AI to scan, analyze, and summarize documents, granting employees fast access to a vast knowledge base, so they can deliver faster, smarter citizen services.

However, without appropriate digital sovereignty, this risks exposing classified, sensitive, and personally identifiable information that must always remain under the organization's control.

The digital sovereignty posture

To avoid exposing sensitive data, the chatbot runs in an **on-premises environment** containing the document database, user interface, and access controls. The organization retains control over data access and storage by using a **dedicated network connection** to a **fully encrypted public cloud environment**.

In addition, **confidential computing** – a technology that creates a secure enclave for data while it's in use – keeps data encrypted and doesn't allow any data to leave the controlled environment or be used for public LLM training.

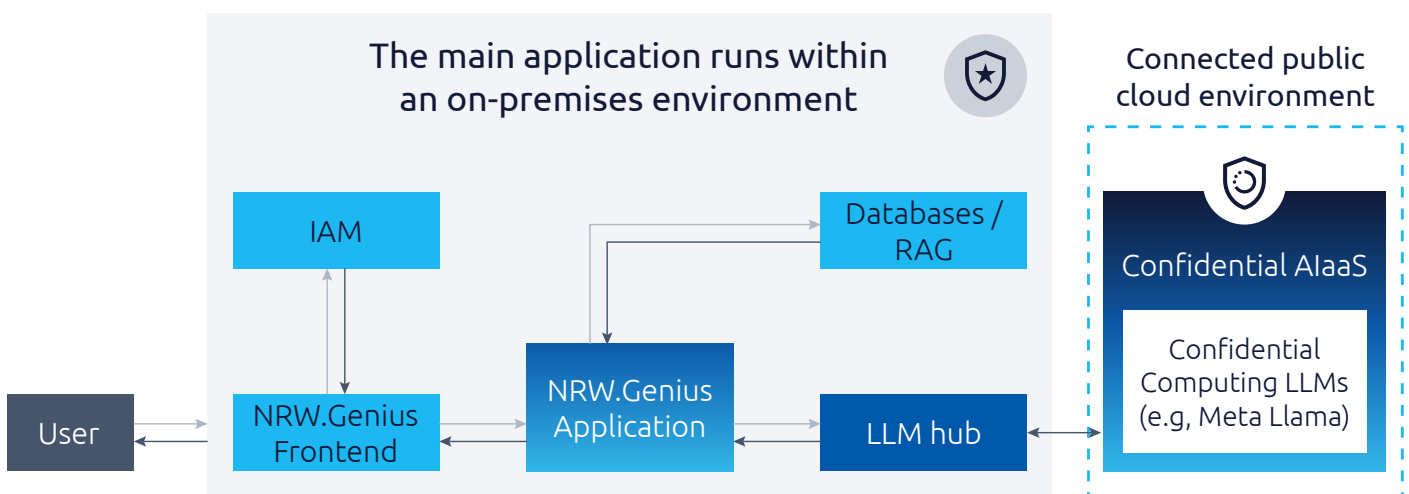


Figure 1: Genius Platform sovereign architecture



2. Building an information-sharing platform for efficient collaboration between police agencies

The scenario

The data protection and privacy conundrum becomes more complex in this scenario, where several police agencies build a platform to share administrative, biometric, and criminal evidence data.

The aim is to enhance crime investigation and prevention processes on a modern cloud platform. But the highly confidential data related to criminal investigations and records typically requires air-gapped, on-premises environments with security-cleared staff and dedicated networks.

The digital sovereignty posture

The platform connects sovereign solutions from public cloud providers with existing on-premises solutions through [secure APIs](#), [shared data models](#), and [common assurance frameworks](#).

[Tiered data classification](#) enables the separation of workloads into multiple 'sovereignty zones' to apply [automated policy enforcement](#) to data at different sensitivity levels. And a [Policy as Code](#) approach bakes data residency rule enforcement into the platform, eliminating the possibility of data being used or stored outside the sovereign environment, even accidentally.

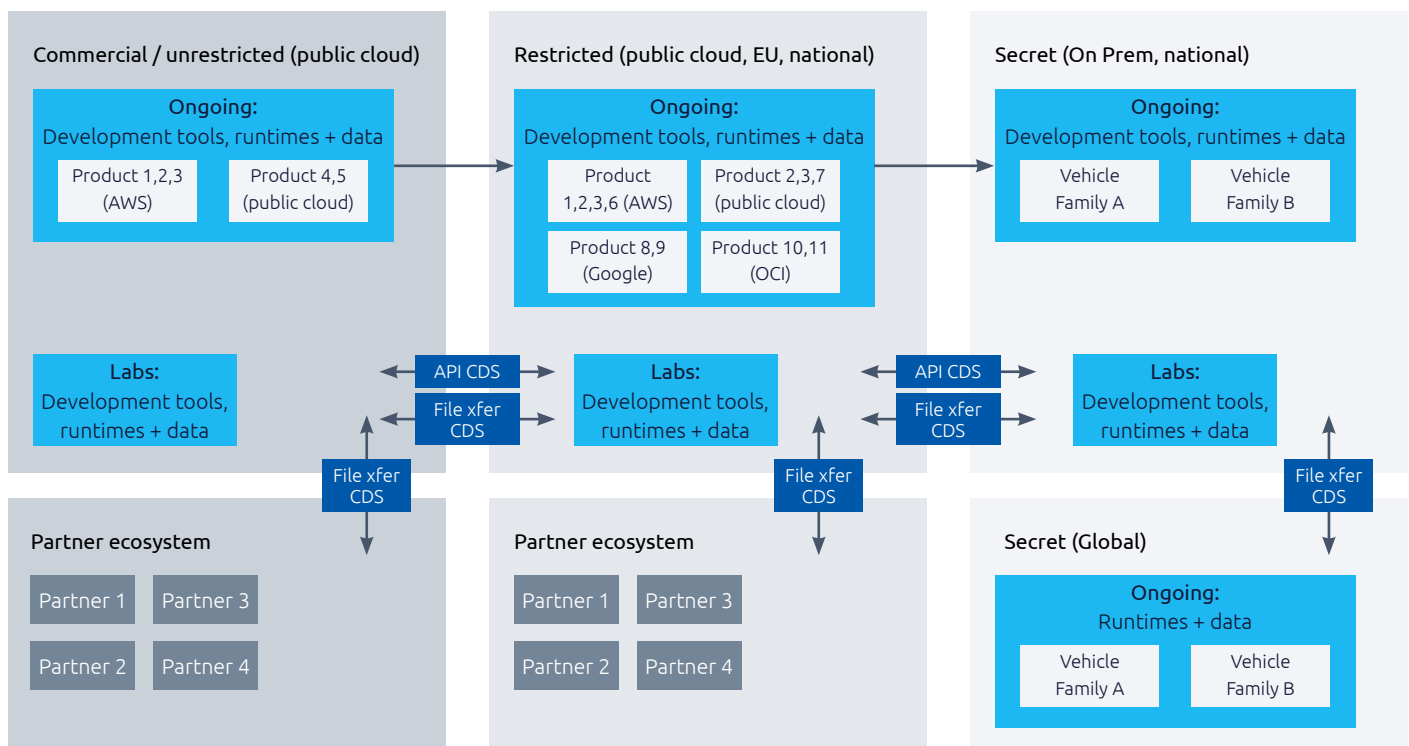


Figure 2 Scenario 2: Police platform concept diagram



3. Creating a multinational tax data exchange platform to secure the future of public finances

The scenario

This scenario expands the digital sovereignty challenge across nations, with multiple tax authorities sharing data to combat tax evasion and fraud, such as in the [EU's VAT in the Digital Age \(ViDA\)](#) program.

But sharing highly sensitive tax data demands a platform that enables interoperability and collaboration while each nation retains control over its citizens' information. Digital sovereignty must be preserved across multiple environments, with secure collaboration zones and shared assurance frameworks.

The digital sovereignty posture

Each nation maintains its own [sovereign enclave](#) – a physically and logically isolated cloud infrastructure aligned with national standards – to retain control over sensitive data, and enable trustworthy collaboration.

A [central collaboration hub](#) allows data marked as shareable to be encrypted and transmitted securely, with [nation-specific protocols](#) govern residency.

In addition, a [multi-cloud architecture](#) balances access and security for data at different sensitivity levels:

- [Public sovereign cloud environments](#) for unrestricted data
- [Domestic sovereign clouds](#) for restricted data
- [On-premises or air-gapped clouds](#) for highly sensitive data





Plot your path to the right digital sovereignty posture

The growing digitalization of government has brought powerful new capabilities to the public sector. But it's also introduced new risks, especially when the availability and integrity of digital services can be controlled or influenced by foreign powers.

With the right sovereignty posture across the entire digital value chain, organizations can protect and assure their digital services. But like any major strategic development in the public sector, establishing the right digital sovereignty strategy is a complex undertaking.

Sovereignty strategies must account for a wide variety of digital use cases, from simple departmental tools to complex multinational programs. That requires partners with the technical expertise, public sector experience, and geopolitical understanding to navigate complexity and co-create sovereign digital solutions that are secure, scalable, and repeatable.

Capgemini supports governments and public sector organizations to define and execute digital sovereignty strategies that protect their operations and data. With a combination of global scale and local sovereignty expertise, we can help you assess your risk, determine the right mitigating actions, and gain control and assurance.

Get started with our [Digital Sovereignty Assessment](#), giving you a structured way to understand the gap between your current risk exposure and your ideal sovereignty posture, so you can begin to formulate a clear sovereignty strategy.

In just 30 days, we'll help you:



Understand your current sovereignty posture and risk exposure



Define an appropriate sovereignty target state



Identify pragmatic next steps to achieve your desired sovereignty levels

And with the assessment complete, we can help you build your strategy and turn it into action, so you can maintain resilient operations and strategic autonomy – and confidently build new capabilities like those in the scenarios in this guide.

Don't wait to be disrupted by the next wave of geopolitical upheaval or new cyber threats. Start regaining control and reducing risk today – [get in touch with our experts](#) to explore your next steps.



Stefan Zosel

VP Cloud Lead Global Public Sector / Sovereign Cloud
stefan.zosel@capgemini.com



About Capgemini

Capgemini is the business transformation partner for enterprises in the age of AI. We help organizations imagine and build an intelligent, sustainable future, combining AI, technology and human ingenuity to transform how they operate, innovate and grow. With unique end-to-end capabilities spanning strategy, technology, engineering and intelligent operations, we bring together deep industry expertise and marketleading capabilities in AI, cloud and data to turn ambition into measurable business outcomes at scale. Supported by a robust ecosystem of partners and nearly 60 years of expertise, Capgemini is a responsible and diverse global organization of over 410,000 team members in more than 50 countries. The Group reported 2025 revenues of €22.5 billion.

Make it real | www.capgemini.com



Make it real .