Digital sovereignty strategies for service providers

Telecommunications service providers are uniquely positioned to become trusted providers of sovereign cloud solutions.

Evolving multicloud architectures must emphasize increased portability, modularity, and security at different levels.

Challenges in an evolving global economy

Geopolitical developments are increasing the focus on digital sovereignty, emphasizing the need for stakeholders to come together and maintain control over their digital assets amid growing data privacy, security, and jurisdiction concerns. This is shaping how nations and organizations control and manage their own and public infrastructure, including how data is stored, managed, and processed with regard to region-specific regulations and priorities.

According to IDC's Digital Sovereignty in Action paper[1], in 2024, 31% of European organizations surveyed said they are currently using sovereign cloud solutions, while 50% plan to do so in 2025. IDC also points out that in 2024, only 15% of organizations cited geopolitical uncertainties as their top driver for using sovereign cloud. Given the rapidly changing political climate in 2025, many organizations have heightened concerns around trust when it comes to choosing and using technology vendors and partners. Digital sovereignty is becoming increasingly important for governments and enterprises.

Telecommunications service providers are uniquely positioned to become trusted providers of sovereign cloud solutions. They have already built essential national digital infrastructure, with their extensive datacenter facilities. Service providers also have the opportunity to deepen established trust with global governments and businesses by continuing to protect sensitive information and enhance cybersecurity. Digital sovereignty is accelerating a global shift towards sovereign cloud adoption and evolving multicloud architectures that emphasize greater portability and modularity at different levels of the architecture. However, achieving this can still be challenging as service providers must:

- Deal with an increased level of complexity. Service providers must offer more granular control of and security for digital assets, operations, technology, and related supply chains.
- Find the necessary funding for building new platforms, infrastructure, and the associated tooling for security and governance.
- Ensure that sensitive data and essential services are shielded from increasing interference and disruption from bad actors.
- Fill a very specific skills gap in their workforce to adhere to diverse and often conflicting national and regional regulations.
- Integrate sovereign cloud operations into existing IT environments and operations.
- Evaluate and select from myriad ecosystem partners to ensure they achieve their own and mandated objectives for trust and control.

1 *IDC InfoBrief, sponsored by Red Hat. "Digital Sovereignty in Action: Building Resilient, Compliant, and Transparent Cloud Ecosystems." Document #EUR153367225, June 2025.*

Governments and enterprises see the incumbent connectivity provider as a trusted entity.

These additional challenges need to be overcome, and service providers can play a key role in providing a sovereign cloud solution. Governments and enterprises see the incumbent connectivity provider as a trusted entity with regard to data security and privacy, and for that data to remain in-country.

Varying regulatory requirements

Compliance with policies and regulations play a critical role in digital sovereignty, which establishes a framework for a complex digital landscape. Service providers are well adapted to navigate and comply with government regulations, but need to understand specific and new regulatory context and frameworks of digital sovereignty to be able to define and implement their own strategy to control risk. Some of the regulatory frameworks that surround digital sovereignty include:

General Data Protection Regulation (GDPR)

GDPR seeks to unify how personal data and privacy is protected online through rules and regulations, as well as punitive sanctions for those who do not comply. Under the terms of the GDPR, any organization that wants to trade with customers in EU countries must abide by a set of data management rules. This includes service providers, no matter where they are based.

Other key regulations include the Digital Markets Act (DMA), Digital Services Act (DSA), the EU Artificial Intelligence Act (AI Act), Data Act, and Data Governance Act. Together, they form a comprehensive framework to safeguard European citizens' data rights and promote digital autonomy.

European Union Artificial Intelligence Act

The AI Act is a comprehensive legal framework to regulate AI within the EU. Using a risk-based approach, AI systems are categorized based on potential harm or compliance with EU regulations. This is to ensure that AI in the EU is ethical, safe, and protects customer data.

European Union Digital Operational Resiliency Act (EU-DORA)

DORA consolidates and upgrades information and communications technology (ICT) risk requirements throughout the financial sector. It provides a common set of standards that mitigate ICT risks for operations. It requires that all participants have the necessary safeguards in place to mitigate and recover from cyber-attacks, ICT-related disruptions and threats, and other risks. DORA introduces an oversight framework for critical third-party providers, such as cloud service providers.

Network and Information Systems Directive (NIS 2)

The NIS 2 Directive moves away from the distinction between operators of essential services and digital service providers (as they were defined in NIS 1) and instead distinguishes between essential entities and important entities. Essential entities include those in the following sectors:

- Banking
- Energy
- Transport
- Health
- Cloud computing
- Domain name system services

- Datacenter services
- Public administration
- Space

Important entities include providers of digital services (including online marketplaces, search engines, and social networking services), as well as entities in food, medical device, pharmaceutical, and motor vehicle sectors.

Directive on critical infrastructure resilience (CIR)

The CIR obliges EU member states to take certain measures to ensure that internal markets provide essential maintenance services for vital societal functions and economic activities. These obligations for critical entities enhance their resilience and improve their ability to provide stabilizing, crucial societal services in the internal market. The CIR also establishes rules for supervising critical entities and provides for the enforcement of those rules.

Cybersecurity Law (CSL), Data Security Law (DSL), and Personal Information Protection Law (PIPL)

Equivalent to the GDPR, the CSL, DSL, and PIPL laws frame China's digital sovereignty approach, jointly governing cybersecurity and data protection.

Strategic goals and dimensions of digital sovereignty

The goal: To deploy and orchestrate scalable, resilient, trusted, interoperable, and reversible infrastructure and services that support open and sovereign requirements.

IDC's Open Source and Digital Sovereignty Come Together paper[2] defines 6 key strategic goals of digital sovereignty:

- Cybersecurity
- Transparent IT operations
- Trusted data management
- Strategic resilience
- Digital economy and skill development
- Interoperability and reversibility

Benefits of working with Red Hat:

- Control where data resides and how it is handled.
- Choose where workloads are deployed, and on what hardware.
- Strengthen business continuity capabilities.
- Respond swiftly to evolving sovereign requirements.

Service providers can achieve these goals by addressing the different dimensions of digital sovereignty. When bringing together digital sovereignty and open source software, service providers will be able to deploy and orchestrate scalable, resilient, trusted, interoperable, and portable (or reversible) infrastructure and services that support open and sovereign requirements.

In this context, reversibility and portability are similar concepts, though not identical. Portability generally refers to the ability to migrate workloads, data, applications, and operations between environments; Reversibility extends beyond environments, and acknowledges the business, legal, and cultural impacts that a migration or vendor change entails. Portability may be considered a subset of reversibility. Note that this is also related to more long-standing concepts of reversibility in thermodynamics, in that they both require the ability to decompose systems into their component parts without losing any pieces.

2 *IDC InfoBrief, sponsored by Red Hat. "Open Source and Digital Sovereignty Come Together." Document #EUR150900123, June 2023.*

Data sovereignty

Data sovereignty encompasses the legal and ethical governance and management of storage, access, management, processing, and the flow of data within a service provider's sovereign borders. A digital sovereignty solution must operate in compliance with local regulations, including privacy laws, data residency requirements, and consent frameworks.

Data governance and management must reflect cultural and societal expectations, particularly when biometric data, healthcare data, or financial information are present. To maintain control over sensitive and critical data, service providers invest in trusted data infrastructures and federated data platforms. To maintain trust, compliance, and competitive advantage, service providers must have a robust cybersecurity strategy that defines who is able to govern the access, analysis, and sharing of data in multicloud and cross-border scenarios.

To address data sovereignty, Red Hat's ecosystem of local and regional partners gives service providers options for storing and processing data locally. These options allow customers to decide where data resides and how it is controlled and handled.

Technology sovereignty

Technology sovereignty includes customer-managed infrastructure, as well as access to—and control over—source code and platforms across the entire technology environment. The ability to independently design, build, and operate systems allows service providers to offer strategic resiliency, a foundational element for public services and competitiveness. Technology sovereignty is often extended towards the supply chain, to mitigate the risk of dominant manufacturers. Adopting a flexible hardware strategy can help reduce vulnerability to risks like geopolitical tensions, export controls, or external platform dependencies.

To address technology sovereignty, Red Hat provides customer-managed infrastructure options that give service providers the flexibility to choose where workloads are deployed, and on what hardware. Additionally, our open source approach provides access to and control over source code, reducing the risk of vendor lock-in and letting service providers adapt technologies to meet their specific needs.

Operational sovereignty

Operational sovereignty brings autonomy over the operation, management, and support of the service provider environment. It includes governance over the authority, skills, and access to operate and maintain sovereign solutions by locally trusted service provider personnel. Many national policies are beginning to mandate that critical digital infrastructure must be supported by staff of specific nationality or within legal jurisdictions, in order to reduce reliance on external managed services and support.

Red Hat's open hybrid cloud solutions and our partner ecosystem strengthen business continuity capabilities, provide a path to operational resilience and transparent IT operations, and give service providers the autonomy needed to manage their environment effectively.

Assurance sovereignty

Assurance sovereignty provides for the independent verification of the integrity, security, and compliance of a service provider environment based on domestic rules, policies, and frameworks. Assurance sovereignty may require service providers to conduct comprehensive audits, assessments, and validations of IT infrastructure, software, and operational practices.

Red Hat solutions and support can help service providers migrate workloads across different cloud providers or on-premise environments, allowing for swift responses to evolving sovereign requirements, and providing interoperability and reversibility. Red Hat makes it possible for service providers to independently verify their infrastructure and assure their prospects and customers that all necessary regulations are being met.

3 key strategies for service providers:

- Strategically invest in sovereign cloud solutions.
- Build advanced AI infrastructure.
- Offer specialized digital sovereignty advisory services.

Figure 1: Red Hat's role with the dimensions of digital sovereignty

Digital sovereignty opportunities for service providers

Digital sovereignty principles and practice offer substantial market opportunities for service providers to take advantage of inherent strengths including their foundational national infrastructure, established trust with governments and businesses, and expertise in managing complex, secure networks. By strategically investing in sovereign cloud solutions, building advanced AI infrastructure, and offering specialized digital sovereignty advisory services, service providers can transcend their traditional role as connectivity providers. This strategic pivot allows them to become indispensable enablers of national digital autonomy, unlocking new revenue streams and re-establishing their strategic relevance in the evolving global digital economy.

European service providers are playing a crucial role in the evolution of digital sovereignty. Their competitive strategies include:

- Direct cloud offerings. By developing and operating their own cloud platforms, service providers can take advantage of existing datacenter infrastructure and network expertise.
- Strategic partnerships with hyperscalers. Providers may collaborate with major global cloud providers to offer trusted or sovereign versions of hyperscaler services. The service provider maintains local operational control, compliance expertise, and network connectivity—combining the scale and innovation of hyperscalers with local sovereignty requirements.

- Connectivity and edge computing. Providers can use their extensive network infrastructure to provide secure, low-latency connectivity to sovereign cloud environments, and develop sovereign edge computing solutions to process data closer to the source within national borders.
- Specialized services. Managed services, cybersecurity solutions, and compliance consulting offers can be tailored to sovereign requirements, with providers acting as trusted advisors and integrators for enterprises and public-sector clients.
- National initiatives. Providers can actively participate in and influence national and EU-level initiatives to shape the future of sovereign digital infrastructure.

By their very nature as custodians of national communication infrastructure, service providers find themselves at the forefront of this profound reorientation. The resilience and security of service provider networks, as well as the ability of a nation to control them, are paramount for achieving comprehensive digital sovereignty. National and regional control is vital for safeguarding national security, protecting critical services, and fostering economic stability.

By strategically investing in sovereign cloud solutions, building sovereign AI infrastructure, and offering specialized digital sovereignty advisory services, service providers can transcend their traditional role as connectivity providers. Specialized assessment and advisory service offerings could include helping businesses identify specific data sovereignty risks, defining appropriate sovereignty frameworks, and implementing compliant cloud architectures.

Service providers will be able to move from commoditized connectivity providers to high-value, strategic digital service providers that directly align with national imperatives. The market demand is clear: Approximately 50% of European organizations plan to adopt sovereign cloud solutions by 2025 to enhance cybersecurity, expand cloud adoption, and meet compliance needs[1].

How open source empowers digital sovereignty

Red Hat's approach to sovereignty is comprehensive, extending beyond pure data protection and providing a framework that helps service providers meet sovereign requirements. By working with Red Hat, service providers gain:

- Trust and transparency. Red Hat's approach to open source software offers inherent transparency, enabling service providers to fully explain, modify, and contribute to the source code without limitation.
- Control and flexibility. Red Hat platforms give service providers the flexibility and choice to build, run, and operate their infrastructure and applications anywhere, in a consistent way.
- Protection and operations stability. Open source technology is key to enhancing digital sovereignty. Its ubiquity within enterprise markets—particularly in areas that are critical to service providers like web serving, networking, and cloud-native environments and applications—means that underlying technologies are broadly supported, standardized, and sustained in ways that create stability while still pursuing progress. This provides the robust yet flexible foundation that service providers need to maintain critical services, protect private data, and recognize and respond to relevant and mandated sovereignty regulation.

Service providers should consider open source and digital sovereignty principles for every strategic sourcing decision that can help incrementally modernize legacy systems. A Red Hat platform foundation provides openness, flexibility, and choice, and equips service providers with the technologies and expertise required to balance enterprises' business needs with nuanced sovereignty requirements.

Learn more about:

- Red Hat's commitment to open source and digital sovereignty.
- Transparent, stable, and flexible Red Hat sovereignty solutions.
- How open source is reshaping the telecommunications industry.

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#2464014_0725