

Microsoft expands sovereign cloud options for government and regulated sectors

Source copy kept by wheresthe.ai for the story "Microsoft expands sovereign cloud options for government and regulated sectors" (<https://wheresthe.ai/d/eu-microsoft-expands-sovereign-cloud-options-for-government-2026-10/>).

Source: <https://blogs.microsoft.com/blog/2026/10/20/advancing-digital-sovereignty-with-greater-control-and-choice>

Text saved 20 Oct 2026 (the page as published).

SHA-256 of the saved text: 1beec913c1f86eb1d4c9725c7ec5bf2e24f3c1724ec46ea4283a9cd59db536a2

Across my conversations with leaders in government, critical infrastructure and regulated industries, one priority consistently rises to the top: putting technology to work on their most important systems while maintaining the control those systems require.

This challenge is becoming more important as advanced cloud and AI capabilities move into public services, regulated processes and essential operations. Organizations are considering more than where data resides. They also seek to understand who can access and operate their systems, how sensitive digital assets remain protected, which technology dependencies matter most and whether critical services can continue as regulatory, geopolitical, security or network conditions change. Digital sovereignty should give organizations greater control and security over the technology they depend on, while continuing to innovate.

Last year, we introduced Microsoft Sovereign Cloud to give customers more choice in how they address these requirements. Since then, we have continued to turn our commitments into practical capabilities across public cloud and customer-operated environments, while expanding how we enable partners to address sovereignty requirements in their local markets. Today, we are sharing the next stage of that work.

A continuum of control, built around the workload

Our approach to digital sovereignty starts with the workload. Each workload carries different requirements for data, operations, technology dependencies, continuity and risk. Microsoft Sovereign Cloud is designed to make it easier for organizations to apply the appropriate level of control to each workload without forcing every application into the same deployment model.

Those needs can vary widely across organizations. A public-facing digital service may benefit from the scale and pace of innovation in the public cloud. A system supporting essential operations may need to continue running locally if connectivity is disrupted. An AI workload handling highly sensitive data may require models, data and processing to remain within a customer-controlled environment.

Microsoft Sovereign Cloud is designed around this workload-based approach, providing a continuum of management, control and options across Sovereign Public Cloud, Sovereign Private Cloud and the Sovereign Partner Ecosystem. Organizations can apply the level of control appropriate to each workload while maintaining a consistent approach to governance and operations across their digital estate. Sovereign Public Cloud adds capabilities for workloads that require greater control and transparency while continuing to benefit from the scale and innovation of Azure.

Sovereign Private Cloud extends cloud capabilities into customer-operated environments, including connected and disconnected operations. The Sovereign Partner Ecosystem broadens the continuum through independently operated environments, specialized partners, locally relevant expertise and technologies that support customers' sovereignty requirements.

These are not isolated destinations. Customers can combine public cloud, private cloud and partner capabilities across their digital estate, applying different levels of control to different workloads as their operating needs evolve.

Making control more visible in Sovereign Public Cloud

For many workloads, the public cloud provides a combination of scale, innovation, integrated security and compliance. Organizations can benefit from these capabilities while applying additional sovereignty controls for residency, confidentiality, operator access, policy and continuity. Our work in Sovereign Public Cloud makes these controls easier to understand, apply and demonstrate.

Sovereign Control Panel , entering public preview at Microsoft Ignite, brings these signals together in a unified Azure portal experience. It helps organizations understand their sovereignty posture, apply and manage controls, identify gaps and risks and take action to address them. It also supports business continuity readiness by helping customers understand workload dependencies and assess portability across operating environments when required.

This visibility complements controls across the operator-access lifecycle. Just-in-time Access and Customer Lockbox give customers additional control over access to their environments. For customers in the European Union (EU) and the European Free Trade Association (EFTA), we are rolling out Data Guardian , which adds European-resident oversight by a trusted EU partner for qualifying Microsoft engineer remote access to in-scope production systems. Production Touch Ledger , also launched with phased rollout in the EU and EFTA, creates tamper-evident records of that access and the actions performed.

Azure Key Vault Managed Hardware Security Module (HSM) already gives customers dedicated, single-tenant protection and control over the encryption keys used by supported Azure services. Last year, we committed to extending that control beyond Microsoft infrastructure. External key management with Azure Managed HSM is now generally available, allowing customers to keep the root encryption key in hardware they own and operate on-premises or through a trusted third party. This gives organizations another option for workloads that require physical control of key hardware outside Microsoft infrastructure.

Azure confidential computing helps protect supported data while it is processed in a hardware-based and attested trusted execution environment. We are also increasing transparency into the technologies that underpin that trust. Azure Confidential Clean Rooms , now in limited preview, applies confidential computing to approved multiparty collaboration, allowing participants to analyze shared sensitive data while limiting broader exposure of the underlying information.

Together, these capabilities provide additional technical and operational controls that can support a broader digital sovereignty strategy aligned to an organization's legal, policy, security, resilience and business requirements.

Designing for resilience and operational independence

For some workloads, digital sovereignty also means maintaining critical operations as connectivity, geopolitical and operating conditions change. Resilience must be designed from the start so essential workloads can continue operating through disruption.

To help customers prepare for these scenarios, we are publishing new sovereign business continuity guidance and architecture patterns . These resources help organizations translate resilience requirements into architectures they can plan, implement and test before they are needed.

For many workloads, the scale and geographic reach of the public cloud provide a strong foundation for resilience across locations and operating conditions. For workloads that require greater operational independence, Sovereign Private Cloud extends that continuum into customer-operated environments. It supports connected and disconnected operating models. The ability to transition workloads from connected to disconnected operations is entering public preview, giving organizations greater flexibility to sustain critical services as connectivity and operating requirements change.

Bringing more of the application lifecycle under local control

Operational independence requires more than infrastructure. Increasingly, organizations need data, development tools, model capabilities and productivity services their applications depend on to operate within the same customer-controlled environment.

Sovereign Private Cloud, built on Azure Local, extends Microsoft cloud capabilities into environments that customers operate and control. SQL Server on Azure Local is already generally available for connected and disconnected deployments. DocumentDB and Blob Storage on Azure Local are both entering public preview, giving organizations more choice in how they run and manage critical data within customer-controlled environments.

GitHub Enterprise Local will become generally available at Microsoft Ignite as a validated GitHub Enterprise Server appliance on Azure Local, helping organizations keep repositories, code and development artifacts under local control. Developers can also use GitHub Copilot with locally hosted models for inference, bringing AI-assisted development closer to their code and data within the environments they control.

The local application environment is expanding with Foundry Local . At Ignite, Foundry Local will become generally available for connected and disconnected operations on Azure Local, with an expanded model catalog that includes Microsoft, partner, open-weight and open-source models. Local inference and agentic retrieval will also enable users to interact with local enterprise data using natural language and receive responses grounded in that data. Integration with Microsoft 365 Local , available in preview for approved customers, extends this functionality to locally operated Microsoft SharePoint and Exchange servers.

Confidential virtual machines on Azure Local are generally available, extending confidential computing capabilities to customer-controlled infrastructure. Hardware-encrypted memory and hardware-based isolation help protect sensitive data while it is being processed. Workload attestation adds assurance before sensitive data or keys are released. For regulated, sensitive and mission-critical workloads, these safeguards provide another layer of protection while giving organizations greater control over where their data and applications run.

Azure Local will support multitenancy , allowing organizations to separate resources, governance and management across multiple tenants while sharing the underlying infrastructure. This significantly expands what customers with distinct business units or security boundaries can achieve with Sovereign Private Cloud. Multitenancy also creates new opportunities for local operators and service providers to deliver differentiated sovereign cloud services on Azure Local infrastructure.

These additions bring more of the application lifecycle under local control, spanning data, development, productivity, AI and operations. Organizations can determine what runs locally based on the requirements of each workload.

Extending the continuum through partners

Navigating sovereignty is increasingly complex. Regulatory, security, operational and business requirements vary across countries, industries and workloads. Organizations must translate these needs into technology and operating models that work in their local context. Meeting these needs often requires a combination of technology, local operating authority, sector expertise and specialized solutions.

The Sovereign Partner Ecosystem broadens the ways customers can address these requirements. National Partner Clouds , including Bleu in France, provide independently operated environments for customers that require a different ownership and operating model. Software partners can enhance Azure Local environments with capabilities across security, identity, observability, backup and recovery, migration, data, networking and applications. Digital sovereignty specialized partners combine Microsoft technologies with local knowledge and implementation expertise. Platform co-innovation partners expand infrastructure choice from datacenter to the edge.

This ecosystem gives customers the flexibility to combine technology, operating models and trusted expertise based on the requirements of each workload.

The next chapter of digital sovereignty

AI is amplifying both the opportunity and the impact of technology choices. As AI systems and agents interact with sensitive data, business processes and essential infrastructure, they also expand the security considerations organizations need to manage. Organizations need clear control over where these systems run, who can operate them, what actions they can take and how critical services continue when conditions change.

Microsoft Sovereign Cloud brings these choices together as a continuum of control across the public cloud, customer-operated environments and our partner ecosystem. It gives organizations the flexibility to apply the appropriate level of control to each workload while continuing to benefit from cloud capabilities and ongoing innovation.

We will continue to expand this continuum so organizations can innovate with cloud and AI while maintaining the control, confidentiality, resilience and operational authority their most important workloads require.

Douglas Phillips leads global engineering efforts for Microsoft's specialized, sovereign and private clouds. He is responsible for Microsoft's global strategy, products and operations that bring Microsoft's industry-leading solutions, including Azure, our adaptive cloud portfolio and Microsoft 365 collaboration suite, to customers with additional sovereignty, security, edge and compliance requirements.

[Learn more](#)

Microsoft Sovereign Cloud

Sovereign Landing Zone architecture guidance

Sovereign Public Cloud Tech Community blog

Sovereign Private Cloud Tech Community blog

Tags: Azure , Azure Local , Foundry Local , Microsoft 365 Local , Microsoft Sovereign Cloud , Sovereign Private Cloud , Sovereign Public Cloud