Microsoft

Microsoft Sovereign Cloud in Europe

October 2026



Notices

This whitepaper provides a detailed overview of Microsoft Sovereign Cloud, Microsoft's comprehensive approach to digital sovereignty for governments, public sector organizations, and enterprises operating in highly regulated or critical sectors. It explains how Microsoft delivers sovereignty through technical architecture, operational governance, and legal commitments without fragmenting the cloud platform or limiting access to innovation.

This document is intended for external audiences, including customers, regulators, and policy stakeholders. It is provided for information purposes only and does not create contractual commitments.

Contents

Introduction 04

Our design approach 05

- Sovereign Public Cloud
- Sovereign Private Cloud
- Sovereign Partner Ecosystem

Microsoft’s European operations 14

- Entity structure
- Corporate governance and access controls
- Legal and contractual commitments for access requests
- Sub-processors and transparency

Turning digital sovereignty into action 17



Introduction

At Microsoft, we believe customers should never have to choose between sovereignty, security, and innovation. Microsoft Sovereign Cloud is designed as a complete portfolio delivering world leading sovereign controls across public, private, and a partner ecosystem that includes nationally governed partner clouds where country-specific regulations demand independent ownership and control.

As cloud computing, data, and artificial intelligence become foundational to economic competitiveness, public services, and national security, governments and enterprises are increasingly focused on who controls and accesses their digital infrastructure, data, and critical systems. This shift has brought digital sovereignty to the forefront of strategic decision-making. Across Europe, these technologies now underpin everything from public administration and healthcare to financial markets, manufacturing, and supply chains. As a result, questions of control, governance, and applicable legal frameworks have moved firmly to the boardroom and cabinet level.

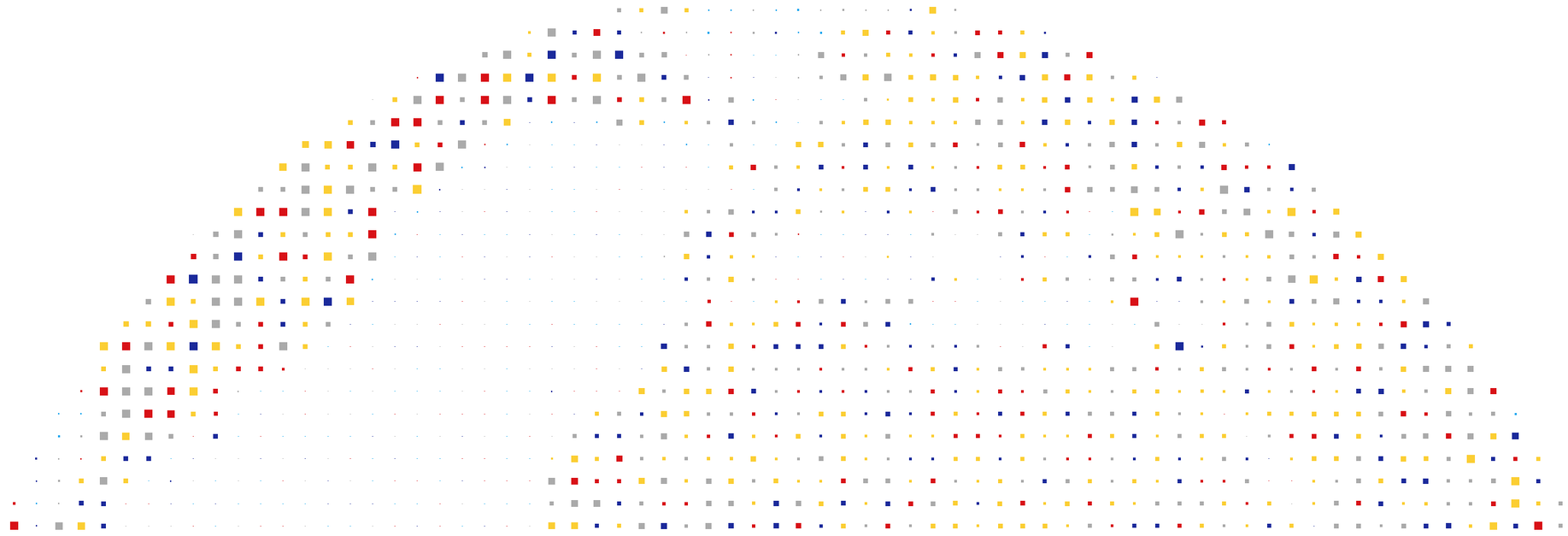
Microsoft delivers secure, resilient, and comprehensive **global infrastructure**, spanning more than 80 datacenter regions and operating across more than 500 datacenters globally that supports customers with a continuum of sovereign controls. Built into this infrastructure are controls that allow organizations to apply the right level of sovereignty for each workload across public, hybrid, to fully disconnected or locally governed environments when required. By embedding protection at every layer of the cloud, Microsoft enables customers to run critical workloads with confidence, helping to maintain control over data, access, and
operations to meet the most stringent security and compliance requirements.

Building on more than 40 years of history as a company in Europe, Microsoft has made sustained, long-term investments to ensure that this global infrastructure is built, operated, and governed in alignment with European values, laws, and expectations. These **investments** include continued expansion of cloud and AI infrastructure across European Union and EFTA member states, strengthening regional resilience, capacity, and redundancy while supporting Europe's digital and economic growth.

At the same time, Europe faces a rapidly evolving regulatory landscape, rising cyber threats, and increased geopolitical uncertainty. Organizations are under growing pressure to innovate responsibly by adopting cloud and AI technologies while ensuring that their data, operations, and intellectual property remain protected under European law. These pressures extend beyond the public sector to operators of critical infrastructure and highly regulated industries including financial services, healthcare, energy, telecommunications, and manufacturing. For many organizations, digital sovereignty is no longer a theoretical concept; it is a practical requirement that cloud providers must address technology, operations, and governance.

In April 2025, we reaffirmed and deepened our long-term commitment to Europe through the announcement of our **European digital commitments**, reinforcing and expanding a set of binding legal, technical, and operational assurances designed specifically to address these concerns. These commitments build on more than a decade of investments in privacy, security, compliance, and resilience, including GDPR readiness, longstanding transparency practices, and the EU Data Boundary for the Microsoft Cloud. Together, they reflect Microsoft's role as critical infrastructure for Europe and the responsibility that comes with it to operate in a way that supports European legal frameworks, regulatory expectations, and values.

Microsoft Sovereign Cloud builds on this foundation by translating Microsoft's global scale, investments in Europe, and the European digital commitments into practical, configurable sovereignty capabilities for customers. Rather than isolating customers into separate or reduced-functionality environments, we provide sovereignty directly into the Microsoft Cloud through built-in controls, flexible deployment models, and legally enforceable commitments. This approach enables organizations to meet evolving sovereignty requirements while continuing to benefit from the power, security, and innovation of the Microsoft Cloud while maintaining compliance, control, and trust.



5 key takeaways from the whitepaper

1. **You aren't locked into a single approach**
   Choose flexible deployment options that adapt and evolve over time

2. **Choosing sovereign doesn't mean slower innovation**
   Run modern cloud and AI at scale and still meet your requirements – no trade-offs for performance, capability, speed

3. **Enforcement is delivered through layered controls**
   Protection through technical, contractual, and operational controls

4. **Control applies at the workload level**
   Individual workloads and tenants can be protected – not just entire regions

5. **It's backed by European law and governance**
   Reinforced through legal frameworks, oversight, and accountability

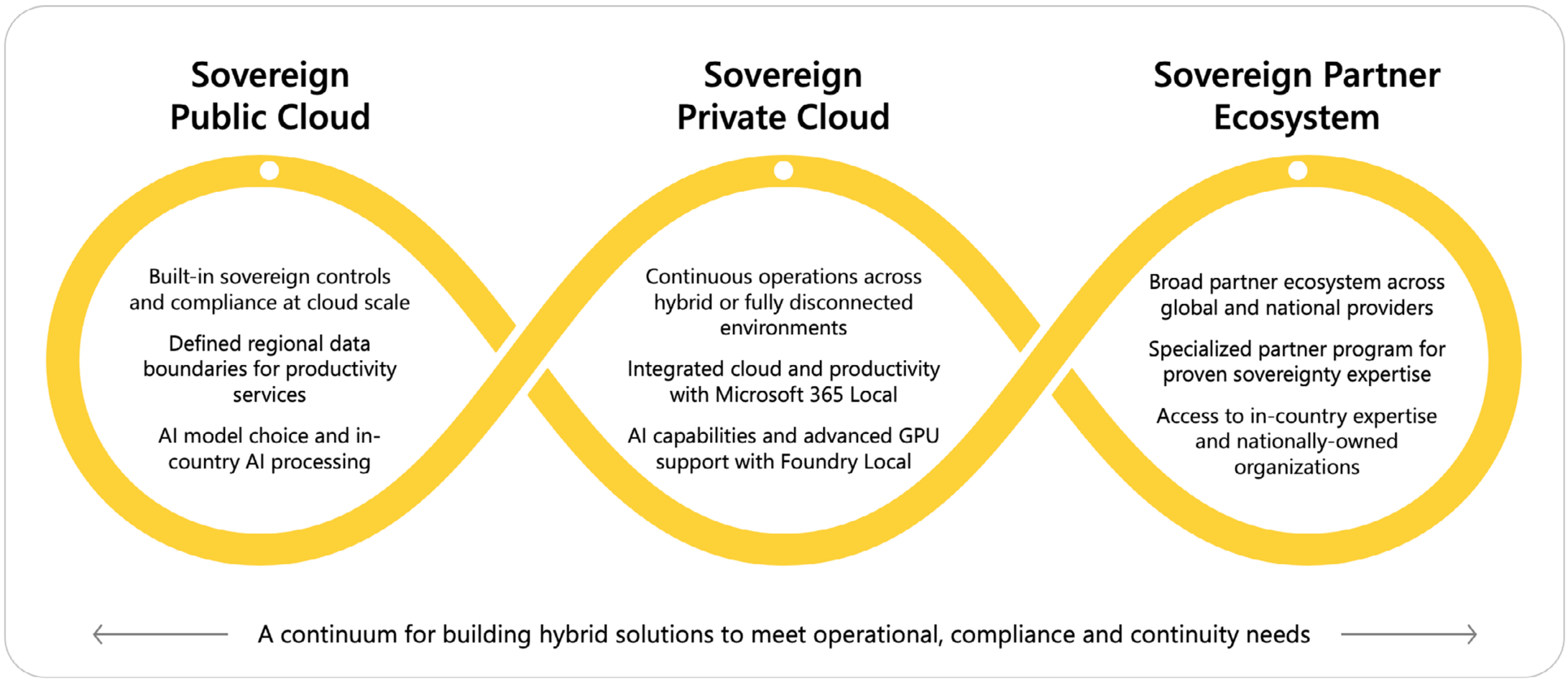
Our design approach

Our approach is simple. Digital sovereignty is foundational to our cloud and services, delivered through a well-governed combination of technical, contractual, and operational controls, and because every workload and every organization have different levels of sensitivity and criticality, sovereignty requirements are adaptable to the needs of each customer.

The Microsoft Sovereign Cloud brings together AI, productivity, security, and cloud workloads to span public, hybrid, and disconnected environments so customers can apply the right level of control, capability, and compliance based on the sensitivity and criticality of each workload rather than relying on a single deployment model.

Microsoft Sovereign Cloud

Most comprehensive set of sovereignty solutions across AI, productivity, security and cloud platform



Sovereign Public Cloud

Building on our experience delivering sovereignty solutions that meet the needs of public sector and highly regulated customers, our Sovereign Public Cloud is the only cloud provider to offer full stack capabilities across AI, productivity, security, and cloud platform for European customers across our existing European datacenter regions

With Sovereign Public Cloud, customer data (including data processed by AI services whether at rest or in transit) stays in Europe, under European law, with operations and access controlled by European personnel, and encryption that is under full control of customers. This is enabled for all customer workloads running in our European datacenter regions **requiring no migration.** Organizations do not have to move to a separate cloud, redesign their environments, or change their architectures to meet their sovereignty requirements; they can apply sovereign controls within the environment they already operate.



EU Data Boundary for Public Cloud environments

Since 2023, Microsoft has operated a comprehensive **EU Data Boundary** to store and process customer data for European Union (EU) and European Free Trade Association (EFTA) countries within Europe, except where customers explicitly configure services otherwise. This commitment is designed to give customers clear control over data location while supporting compliance with EU and Member State data protection requirements.

Under the EU Data Boundary, Microsoft keeps customer content - such as files, emails, documents, and application data - within EU/EFTA datacenters for covered services including Microsoft 365, Azure, Dynamics 365, and Power Platform. Customers retain the ability to configure data movement or enable cross-region scenarios where required for their business operations.

In addition to customer content, Microsoft's EU Data Boundary extends to service-generated data, including pseudonymized personal data, system logs, telemetry, and professional services data generated during support interactions. With the completion of the final phase of the EU Data Boundary, this category of data, often overlooked in residency discussions, is also stored within the EU/EFTA for in-scope services (this does not include billing data). This reduces cross-border data flows and supports a more comprehensive residency posture than models that focus solely on customer-created data.

Microsoft's data boundary commitments also include AI data processing. For eligible services such as Microsoft 365 Copilot, prompts and responses are processed within the EU Data Boundary for customers residing in EU/EFTA and Microsoft is expanding in-country AI data processing options to further localize processing where required.

Microsoft works closely with customers, regulators, and data protection authorities to provide clear documentation, transparency reports, and contractual commitments describing data handling practices and the controls used to enforce the EU Data Boundary. This approach provides customers with the ability to assess and demonstrate compliance while continuing to benefit from the scale, security, and innovation of the Microsoft Sovereign Cloud.

Technical controls

Microsoft implements defense-in-depth technical controls that reduce reliance on operator trust and give customers verifiable, encryption-based control over their data. This includes:

Sovereign landing zone (SLZ) for policy-driven governance and deployment

Built on the Azure landing zone (ALZ) foundation, the Sovereign landing zone provides prescriptive, scalable reference architecture and tooling for operationalizing digital sovereignty in Azure. SLZ applies governance and compliance requirements from the outset with the latest updates including an enhanced management group hierarchy and built-in Azure Policy definitions, initiatives, and assignments aligned to Sovereign Public Cloud control levels. SLZ includes guidance for deploying key services, such as Azure Key Vault Managed HSM where required, to support higher levels of sovereign control. Deployment is streamlined through Azure landing zone accelerators, Infrastructure-as-Code (IaC), and reusable libraries, enabling organizations to apply sovereign controls consistently across environments.

Hardware-based isolation and protection of data in-use

At the infrastructure level, Microsoft provides Azure Confidential Computing, which protects data while it is being processed by executing workloads inside hardware-based Trusted Execution Environments (TEEs). These environments are designed so that data remains encrypted in memory and inaccessible to cloud operators, administrators, or other software processes outside the enclave. Customers can use remote attestation to validate the integrity of the hardware and software stack before workloads are allowed to run, ensuring that only trusted environments can process sensitive data.

Key-based customer control over data access

Microsoft further constrains access through customer-controlled encryption. With Customer Managed Keys, Azure Key Vault Managed HSM, and External Key Management, customers retain control of the encryption keys used to protect their data. Because Microsoft does not possess these keys, we cannot independently decrypt customer data. In the event of a lawful government access request, any data provided would remain encrypted, with the ability to unlock it resting with the customer.

Operational oversight, visibility, and auditable access

For operational scenarios where limited access is required to maintain service reliability, Microsoft enforces strict access controls with customer visibility. Customer Lockbox requires explicit customer approval before Microsoft personnel can access customer content during support incidents. For European sovereign operations, Data Guardian adds European personnel approval and records privileged access actions in tamper-evident logs, enabling post-event review and regulatory audit. Sovereign Control Panel provides a unified experience for monitoring and evaluating sovereignty controls and operational posture across cloud environments. Access paths are authenticated, authorized, and logged, and tooling is designed to make privileged access both exceptional and traceable, rather than implicit.

Transparency and logging

Microsoft provides comprehensive logging and auditing capabilities across its cloud services, allowing customers to monitor administrative actions, access attempts, and data operations. Audit records are protected to prevent unauthorized modification and are available to support internal governance and external regulatory review. Microsoft's contractual commitments further reinforce these technical measures by requiring logging, access justification, and customer notification as part of its operational controls, ensuring that technical safeguards are complemented by enforceable obligations.



Sovereign Public Cloud roadmap

Enhanced Sovereign Control Panel capabilities

will expand organizations' ability to discover, control, and act on sovereignty requirements through centralized visibility into sovereignty posture, policy controls, operational governance, and compliance status. New capabilities will help organizations assess sovereignty requirements, monitor adherence to controls, and take action across cloud environments from a unified experience.

Expanded confidential computing capabilities for Sovereign Public Cloud

will strengthen protection for data in-use through hardware-based isolation and trusted execution environments, enabling a broader range of sensitive cloud and AI workloads to benefit from confidential computing protections.

Expanded Sovereign landing zone capabilities

introduce Infrastructure-as-Code support with Bicep, enabling organizations to deploy and operate sovereign workloads at scale through automated policy enforcement, governance controls, and compliant-by-design architectures. This helps accelerate deployment, reduce compliance complexity, and maintain visibility into sovereignty posture across cloud environments.



Sovereign Private Cloud

For customers with workloads that have specialized needs, Sovereign Private Cloud brings Microsoft's cloud, productivity, and AI services into customer-owned and operated environments. Azure Local provides the infrastructure foundation, bringing Azure services and cloud-consistent management to on-premises and edge environments, enabling organizations to run virtualized workloads, containers, and Azure services locally while maintaining operational control through Azure Arc.

On this foundation, organizations run the Microsoft services they depend on, entirely within their own infrastructure. Teams work in familiar productivity and collaboration tools with Microsoft 365 Local and Azure Virtual Desktop. Developers build and ship software with GitHub Enterprise Local, keeping source code and DevOps workflows within the sovereign environment. Operational data stays local with SQL Server and other relational and document data services. And with Foundry Local, organizations run AI models, tools, and agents directly against that data, so sensitive information never has to leave the sovereign environment. Customers run their own applications alongside all of it on general purpose virtual machines and AKS.

Building on Microsoft's decades of experience delivering on-premises and hybrid technologies to governments and regulated industries, Azure Local runs with or without cloud connectivity, scales from single node to data center size deployments, and gives organizations control over where their data lives and who can access it. While enabling data residency, regulatory compliance, and low latency performance, Azure Local enables industry-leading capabilities in cloud-connected, intermittently connected, or fully disconnected environments to meet customer resiliency and business continuity requirements, even in highly regulated or edge scenarios.

Connected environments

Sovereign Private Cloud supports connected and intermittently connected environments. allowing organizations to extend Microsoft cloud services into customer-controlled infrastructure while maintaining consistent management, security, and compliance capabilities. Using Azure Local, customers can operate workloads across on-premises and cloud-connected environments with a unified control plane, enabling data residency, low-latency processing, and operational autonomy where required. This hybrid model is particularly well suited for regulated industries and public sector organizations that must balance innovation and scalability with localized control and regulatory alignment.

Disconnected environments

For scenarios where connectivity to the public cloud is limited or not permitted, Sovereign Private Cloud supports fully disconnected operations. In these environments, customers can run cloud services with an entirely on-premises control plane, allowing systems to operate securely and independently without reliance on external network access. Disconnected deployments are designed to support mission-critical workloads, edge scenarios, and sensitive environments where regulatory, security, or resilience requirements necessitate isolation, while still benefiting from Microsoft-validated infrastructure, updates, and lifecycle management processes.

Sovereign Private Cloud roadmap

Disconnected high scale deployments *(in preview)*

will extend scale points to support large-scale Azure Local deployments with a disconnected control plane. This means customers will be able to expand from single-node and cluster deployments to disconnected multi-rack and data center environments.

Expanded sovereign AI capabilities *(in preview and upcoming)*

will broaden the range of models organizations can run locally through Foundry Local and add retrieval and agentic experiences, so teams can build AI applications grounded in their own information entirely within the sovereign environment.

Expanded data services *(in preview and upcoming)*

will extend the range of data services organizations can run in customer-controlled environments, including fully disconnected, so transactional, document, and application data workloads can sit alongside the AI and applications that depend on them.

Expanded confidential computing for Sovereign Private Cloud *(upcoming capability)*

will extend hardware-based protection for data in use to customer-controlled environments, enabling sensitive workloads and models to run with confidential computing protections on-premises.

Enhanced change controls *(upcoming capability)*

will introduce configurable policies and approval workflows to give organizations explicit oversight of updates and configuration changes as they propagate from cloud-connected environments to customer-controlled infrastructure, strengthening governance and compliance.

Site-to-site disaster recovery *(upcoming capability)*

will be an expansion of Azure Site Recovery capabilities for Azure Local to support business continuity by keeping applications and workloads available during infrastructure failures or localized outages.

Move from connected to fully disconnected *(upcoming capability)*

will continue support for flexible deployment models that allow customers to move workloads from connected environments to fully disconnected operations, enabling greater autonomy and resilience as operational or regulatory requirements evolve.



Sovereign Partner Ecosystem

Sovereignty outcomes depend not only on where data resides and how it is protected, but on who designs, operates, and legally governs the environment in which it runs. The Sovereign Partner Ecosystem addresses this dimension. It extends Microsoft Sovereign Cloud through partners who deliver and operate solutions in-country, a specialization that identifies validated sovereignty expertise, a marketplace of partner software and services, and, where national requirements demand it, cloud environments that are independently owned and operated by national partners. Together these elements support the first of Microsoft's European digital commitments: to help build a broad AI and cloud ecosystem across Europe.

Global sovereignty partners

European organizations rarely adopt sovereign cloud in isolation. Most are modernizing systems already in production, migrating regulated workloads, and integrating national identity, security, and archiving requirements. This work depends on partners with local presence and sector knowledge.

Microsoft's partner ecosystem spans global systems integrators, regional and national service providers, independent software vendors, and managed service providers, including organizations that are nationally owned and governed. Customers gain access to in-country expertise, local language support, and local contracting arrangements. The underlying platform remains consistent, while delivery, operations, and accountability are adapted to the requirements of each jurisdiction.

Digital Sovereignty specialization

For sovereign workloads, the selection of a delivery partner is itself a control decision. To make that decision verifiable, Microsoft offers the Digital Sovereignty specialization within the Microsoft AI Cloud Partner Program.

Partners holding this specialization have demonstrated proven expertise in delivering secure, compliant, and locally governed solutions across Azure and Microsoft 365, including data residency, operational access controls, encryption and key management, and the regulatory frameworks that apply to specific sectors. The specialization enables customers to identify qualified partners in advance of engagement. For regulators and internal risk functions, it provides independent evidence that a partner has been assessed against a defined standard rather than relying on self-declared capability.

Partner solutions in the marketplace

Sovereignty requirements extend beyond the platform to the software that runs on it. Through the marketplace, customers can identify partner software and services that extend sovereign cloud capabilities across security, compliance, data, AI, infrastructure, and operations. These solutions are procured through established commercial channels, allowing organizations to assemble a complete environment without operating outside their existing governance model.

National Partner Clouds

In France and Germany, our National Partner Clouds offer fully-featured and independently operated instances of Microsoft 365 and Microsoft Azure under complete national ownership and control.

In France, *Bleu*, a joint venture between Orange and Capgemini, operates a "cloud de confiance" for the French public sector and critical infrastructure providers – designed to meet the French government's (ANSSI) SecNumCloud requirements.

In Germany, *Delos Cloud*, an SAP subsidiary operates a sovereign cloud for the German public sector that is designed to meet the German government's BSI cloud platform requirements.

Most organizations will use a combination of these deployment models because not every workload requires the same level of independence or isolation. Microsoft Sovereign Cloud allows customers to establish the appropriate controls from the outset, so they are prepared to operate under their chosen requirements at any time.



Microsoft's European operations

Microsoft's approach to sovereignty in Europe is grounded in governance under European law, clear legal accountability, and transparent operational controls. Rather than creating an isolated legal entity for sovereign workloads, Microsoft delivers sovereignty outcomes through established European entities, reinforced governance models, and enforceable technical and contractual safeguards.



Entity structure

Microsoft delivers cloud services in Europe through Microsoft legal entities established and operating within the European Union (EU), subject to European law and aligned with region-specific regulatory requirements. These entities are responsible for the operation of European cloud infrastructure and services and contract directly with European customers. Our European datacenter operations are governed by a European board of directors which operates under European law, reinforcing our commitment to local oversight. This structure provides continuity of legal accountability while preserving a consistent cloud platform and service portfolio across regions.

For workloads requiring heightened legal independence or alignment with national sovereignty regimes, Microsoft additionally supports National Partner Clouds, such as those in France and Germany. These environments are independently owned and operated by in-country entities, subject to local corporate governance, national law, and regulatory oversight, while delivering Microsoft technology under strict contractual and operational controls. This model enables customers to meet national requirements without fragmenting their broader cloud architecture.

Corporate governance and access controls

Microsoft enforces sovereignty outcomes through a defense-in-depth governance model that combines technical controls, operational oversight, and legally enforceable commitments. This approach is designed to reduce reliance on operator trust and give customers verifiable control over access to their data.

At the infrastructure level, Microsoft protects data even while it is being processed, helping ensure that sensitive information cannot be accessed by cloud operators unless explicitly authorized. These protections are designed to keep customer data isolated and protected throughout its lifecycle, complementing encryption when data is stored or transmitted and reducing exposure to unauthorized access, even in highly privileged operational scenarios.

Microsoft further limits access through customer-controlled encryption. With options such as Customer-Managed Keys and External Key Management, customers retain authority over the keys that protect their data. Without those keys, Microsoft cannot independently read or use customer content, ensuring that access decisions remain under customer control.

In situations where limited operational access is required to maintain service reliability, Microsoft applies strict, auditable controls. Customer Lockbox requires explicit customer approval before Microsoft personnel can access customer content during support incidents. For European sovereign operations, Data Guardian adds European personnel authorization and oversight, with all actions recorded in tamper-evident logs. Together, these measures can ensure that any privileged access is deliberate, transparent, and fully traceable.

Legal and contractual commitments for access requests

Microsoft does not give any government direct or unfettered access to customer data and manages government and law-enforcement access requests through defined legal and operational processes designed to ensure alignment with European law and customer interests. For European cloud services, Microsoft operates under European legal frameworks, and all requests relating to customer data are reviewed individually by trained legal, privacy, and compliance teams with regional expertise. Requests are assessed for jurisdiction, legality, and scope before any action is taken, and those that do not meet applicable legal standards are challenged or rejected.

Consistent with a customer-first posture, Microsoft's contractual terms and privacy commitments are designed to maximize customer control and transparency. Wherever legally permissible, Microsoft redirects requests to customers so they can respond directly or seek judicial review. Where notification is allowed, Microsoft informs customers promptly and provides sufficient detail to enable appropriate action. If notification is legally restricted, Microsoft seeks to lift or narrow such restrictions. Microsoft has also publicly committed to lawfully contest requests that are facially invalid or conflict with law, including extraterritorial demands inconsistent with European legal standards, as reflected in its

European digital commitments and Digital Resilience Promise. Microsoft has a long history of successfully challenging unnecessary secrecy orders, both directly in communications with law enforcement and formally in court.

These legal commitments are reinforced by the technical and contractual controls described above, which limit operator access and reduce exposure to unauthorized disclosure. Together, regional legal accountability, enforceable customer rights, and auditable controls provide customers with confidence that access requests are handled consistently, transparently, and in accordance with European legal requirements.

Sub-processors and transparency

Microsoft maintains transparency around the use of sub-processors and applies contractual, technical, and organizational safeguards consistent with EU data protection and security requirements. Sub-processors are subject to due diligence, contractual obligations, and ongoing oversight to meet Microsoft's standards for security, privacy, and compliance.

Comprehensive logging and auditing capabilities across Microsoft cloud services allow customers to monitor administrative actions, access attempts, and data operations. Audit records are protected against unauthorized modification and support both internal governance and external regulatory review. These technical safeguards are reinforced by contractual commitments requiring logging, access justification, and customer notification, ensuring transparency and accountability are enforceable as well as observable.

Together, Microsoft's entity structure, governance model, and sub-processor controls provide customers with confidence that cloud services in Europe operate under clear legal accountability, disciplined operational oversight, and transparent access controls aligned with European sovereignty expectations.



Turning digital sovereignty into action

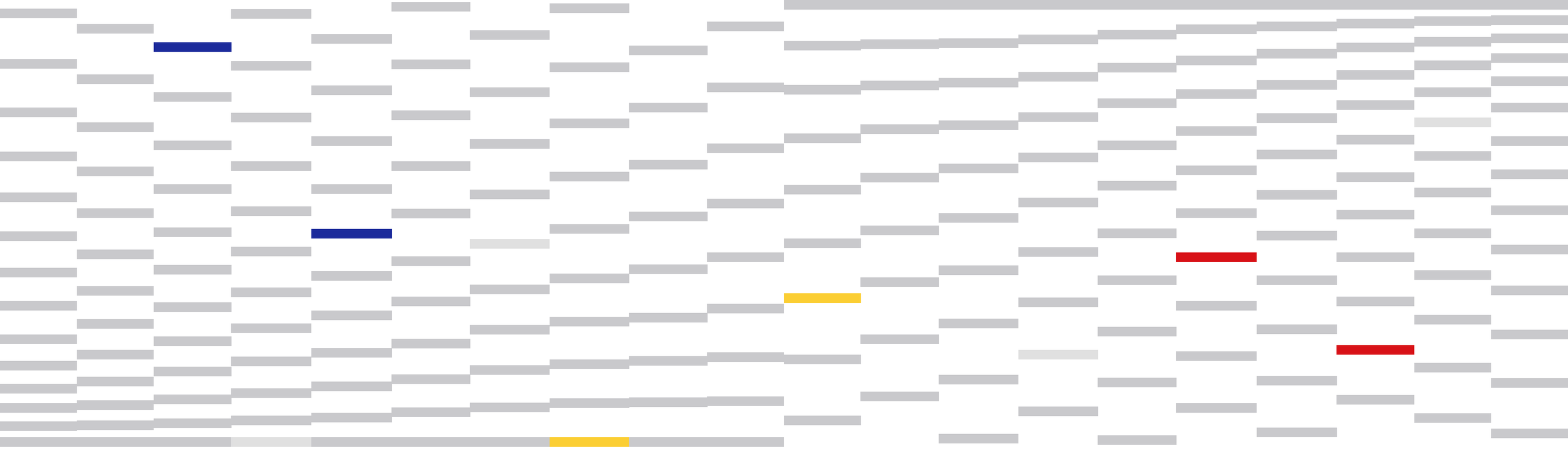
European organizations are navigating a period of profound change. Cloud and AI technologies are reshaping how public services are delivered, how industries compete, and how critical systems operate; all while regulatory expectations, security threats, and geopolitical uncertainty continue to intensify. Meeting these challenges requires more than compliance with today's rules; it requires a cloud platform designed to adapt as requirements evolve.

Microsoft Sovereign Cloud is designed to help organizations take the next step with confidence. Rather than requiring a separate or isolated cloud, Microsoft enables customers to apply sovereign controls across the full Microsoft stack without sacrificing innovation, scale, or functionality.

One way organizations can begin their digital sovereignty journey in the public cloud is through **Sovereign landing zone** (SLZ). Organizations can begin by assessing sovereignty requirements by workload and establishing a Sovereign landing zone as the foundation for secure, compliant cloud and AI adoption. By adopting Sovereign landing zone, customers can gain practical architecture that accelerates alignment with regional sovereignty requirements while supporting scale across Azure regions. Over time, the built-in sovereign policies and controls will continue to expand, helping organizations achieve sovereign outcomes out of the box more quickly and with greater confidence.

Microsoft's commitment is long term. Through continued investment, transparent governance, and legally enforceable assurances, we aim to be a stable and trusted partner for Europe's governments, enterprises, and critical institutions. Microsoft Sovereign Cloud provides a foundation for adopting cloud and AI technologies with confidence while supporting innovation, resilience, and control in an increasingly complex digital landscape.







The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2026 Microsoft Corporation. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.