Microsoft

Microsoft's European Digital Commitments

An Executive Overview

Empowering customers with a multi-tiered strategy to enhance customer choice and control, and strengthen operational resiliency

The geopolitical landscape shaping the coming decades demands a clear and confident response that creates predictability, opportunity, and security.

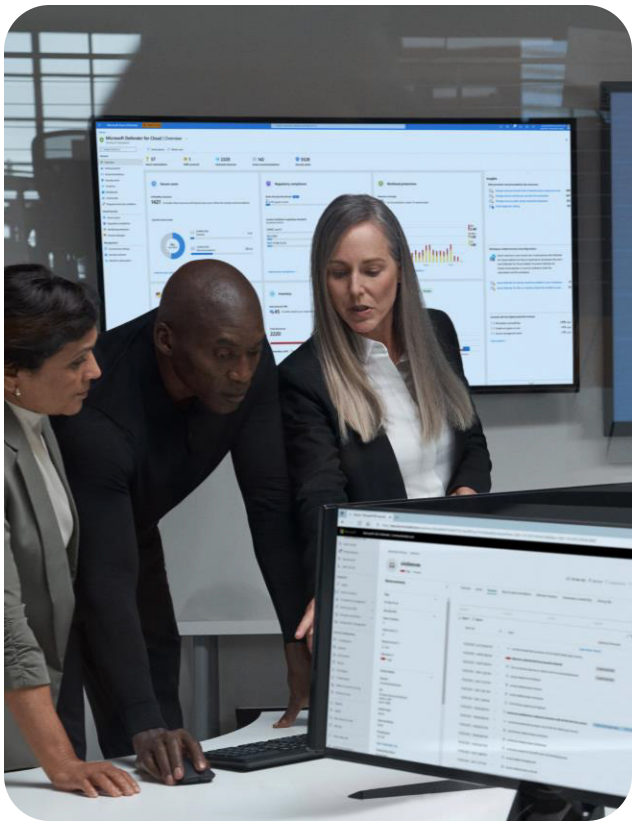
Europe is our vital partner in advancing digital innovation, regulatory leadership, and economic resilience. Our collaboration with European institutions, customers, and governments spans four decades and is built on a deep economic interdependency.

Microsoft's approach to digital sovereignty allows every institution and individual to participate in the digital economy securely, independently, and with self-determined controls to meet a broad set of requirements.

To enhance customer choice and control, and strengthen operational resiliency, we offer a sovereignty continuum across public, private, and national partner clouds. Microsoft Sovereign Cloud delivers a comprehensive, flexible solution for digital sovereignty, empowering organizations of all sizes to innovate at their own pace.

We also continue to invest in digital infrastructure and the skilling of Europeans, always recognizing the need to understand European values, to support European needs, and to comply with European rules.

Microsoft Sovereign Public Cloud



Microsoft's Sovereign Public Cloud integrates sovereignty features into standard public cloud services and optimizes for European data residency and access control.

- Our European datacenter operations are governed by a **newly appointed board of directors** composed exclusively of European nationals and employed by Microsoft Ireland Operations Limited, an Irish company that owns all Microsoft datacenter entities in Europe. This board is effective as of June 26, 2025, and operates under European law, reinforcing our commitment to local oversight.

- Through our **European Union (EU) Data Boundary**, we enable European customers to store and process their data in the EU and the European Free Trade Association (EFTA). We offer customers robust capabilities across the entire stack to give customers control of how their data is encrypted and secured, and who can access it. Our solutions are backed by contractual agreements and include an express promise to challenge any government demand for EU public sector or enterprise data where we have a legal basis for doing so. It also commits us to providing monetary compensation to these customers' users if we disclose their data in response to a government request that violates the EU's General Data Protection Regulation. These measures go beyond the recommendations of the European Data Protection Board.

- **Technical features** enable customers to keep their data and operations secure through built-in sovereign controls, end-to-end confidential computing, and seamless integration of AI and compliance tools.

Sovereign Public Cloud core technical features

Sovereign Landing Zones

Sovereign Landing Zones enforce an opinionated and consistent set of guardrails that is easily configurable and deployable. It gives governments and regulated industries a fast, consistent way to meet evolving sovereignty requirements at scale by enforcing compliant architectures, policies, and controls from day one.

Azure Key Vault

Secure storage of sensitive data such as API keys, passwords, certificates, and cryptographic keys, to give customers full control over their keys and the ability to grant permission for their own and partner applications.

External Key Management

Allows management of encryption keys outside of Azure Key Vault in on-premises hardware security modules or in other third-party cloud providers for organizations with specific compliance or regulatory requirements.

Azure Confidential Computing

Processes data in a trusted environment, and controlled solely by the customer, to prevent data access by cloud providers, administrators, and users while it is being processed. The data is encrypted in a hardware-based environment and processed only after the cloud environment is verified. Customers specify the hardware and software combination that can access their data and their code.

Data Guardian

Provides enhanced operations and access to European Microsoft Cloud services controlled by European residents and tracked by tamper-evident logs. Microsoft's EU Data Boundary already provides an industry-leading commitment to store and process your data on infrastructure located in Europe (EU/EFTA). Data Guardian provides an added layer of human and technical assurance by ensuring that only Microsoft personnel residing in Europe control remote access to systems across Microsoft Azure, Microsoft 365, and all other commercial cloud services. All remote access by Microsoft engineers to systems that store and process your data in Europe is approved and monitored in real time by personnel located in Europe, with every access event recorded in a tamper-evident ledger.

Regulated Environment Management

Allows configuration, deployment, and monitoring of workloads to support sovereign operations through a unified portal.

Microsoft continues to **strengthen cybersecurity protections for European customers and partners** by aligning our work and programs with evolving cybersecurity threats and regulatory requirements. We are also committing to the following additional steps:

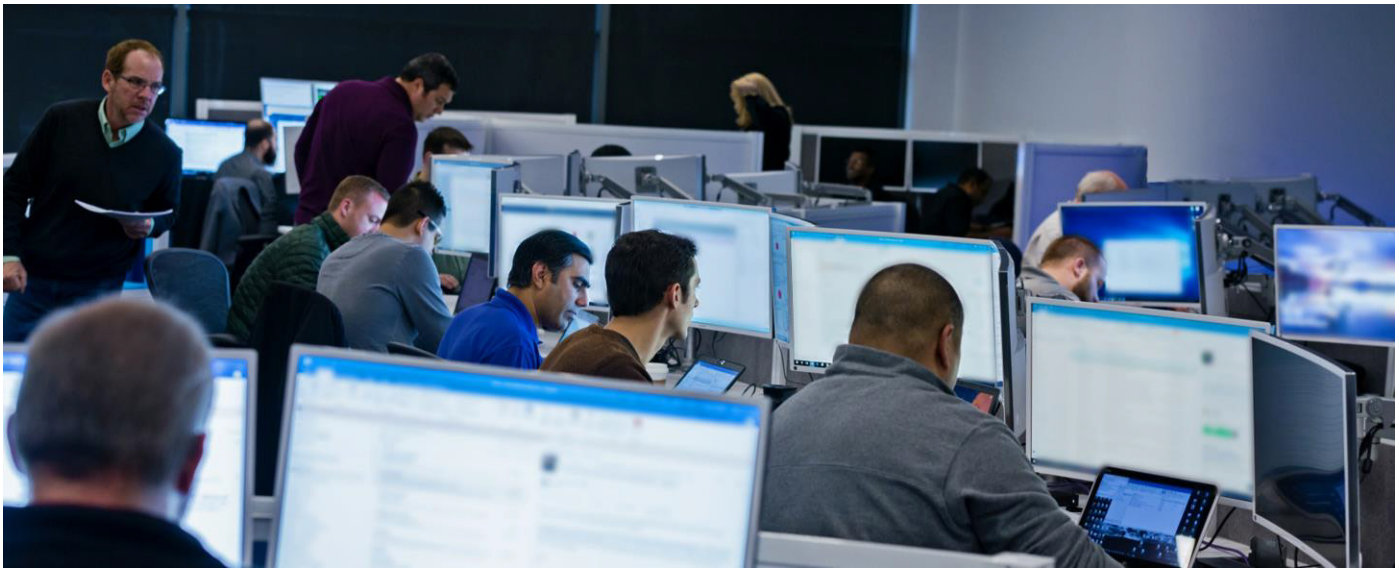
- The appointment of a dedicated **Deputy CISO for Europe** reporting directly to Microsoft's CISO. The Deputy CISO for Europe will be accountable for compliance with current and emerging regulations in Europe, including the Digital Operational Resilience Act, the NIS 2 Directive, and the Cyber Resilience Act (CRA).

- As the CRA reshapes the regulatory landscape, Microsoft is accelerating compliance through its **Secure Future Initiative** and active participation in **the European Commission's Expert Group on Cybersecurity of Products with Digital Elements.** We are engaging with stakeholders on key CRA topics, such as vulnerability reporting, security by design, and open-source security, and sharing innovations to support customer compliance.

- In recognition of the importance of security as the foundation of trust, we will **engage an independent auditor to verify and validate our commitments** to Europe, giving customers added assurance that their digital operations remain secure, compliant, and future-ready.

- Our **European Security Program** puts AI at the center of our work to protect traditional cybersecurity needs.

And importantly, because **Microsoft's public cloud is a sovereign cloud by design**, customers will be able to benefit from all the features and offerings referenced above without the need to migrate their workloads to different infrastructure.



Strengthening protection of digital and AI infrastructure: Three focused elements

AI-based threat intelligence sharing with European governments.

We track the most sophisticated nation-state cyber activity and offer timely insights into evolving global threats, including tracking nation-state activity and monitoring emerging threats from deepfake synthetic media through the Microsoft Threat Analysis Center.[1] We have launched a pilot program with Europol's European Cybercrime Centre (EC3), embedding Microsoft Digital Crimes Unit investigators at EC3 headquarters in The Hague to enhance intelligence sharing and operational coordination.

Additional investments to strengthen cybersecurity capacity and resilience.

We are investing additional resources to further our work with European governments, civil society, and innovators to strengthen local capabilities. We have renewed our three-year partnership with the CyberPeace Institute to support non-governmental organizations, promote accountability for bad actors, and increase digital resilience. A new collaboration with the Western Balkans Cyber Capacity Centre scales cybersecurity in a region where malicious actors have long sought to destabilize countries bordering the EU.

Expanding partnerships to disrupt cyberattacks and dismantle networks.

We are expanding our partnerships with law enforcement and regional actors to disrupt malicious and criminal activity. Our Statutory Automated Disruption Program accelerates the takedown of malicious domains and IP addresses, raising the cost of cybercrime and reducing exposure for organizations operating in Europe.

[1]The European Security Program will be made available to European governments, free of charge, in all 27 EU member states, EU accession countries, EFTA members, the United Kingdom, Monaco, and the Vatican.

Microsoft Sovereign Private Cloud

Microsoft's Sovereign Private Cloud uses dedicated infrastructure for the highest sovereignty needs, while keeping operational consistency with Azure run in disconnected or customer-controlled datacenters.

Azure Local enables compliance with data residency and sovereignty requirements while maintaining a consistent management and developer experience.

Microsoft 365 Local supports national regulatory compliance and sovereignty requirements when running productivity workloads on Azure Local in on-premises or air-gapped environments. It offers a simplified deployment and management framework that enables organizations to run trusted productivity workloads—such as Exchange and SharePoint—on Azure Local within environments fully controlled by the organization.

Microsoft 365 Local also supports on premises or air-gapped environments, or hybrid configurations extending Microsoft 365 cloud services where appropriate.

Customers looking to deploy M365 Local will benefit from the strength of Microsoft's partner ecosystem, including a new Digital Sovereignty Specialization in the Microsoft AI Cloud Partner Program.

Learn more about Azure Local

Ensuring continuity of service

Our legal and operational safeguards maintains service and business continuity in the face of geopolitical volatility, supported by local infrastructure and strategic partnerships.

Our legally binding **European Digital Resilience Commitment** means we will use all available legal means to contest any government order seeking to suspend or cease cloud operations in Europe. This is a contractual obligation supported by our proven record of legal challenge. Our European government customers have this binding contractual commitment in our Data Protection Terms.

To enable business continuity, Microsoft and Delos will establish a **business continuity partnership** to give European public sector and highly-regulated customers the option to migrate to a European-operated fallback environment in the unlikely event that Microsoft is legally restricted by a non-European government from providing cloud services to customer and ceases to do so as a result.

Delos Cloud Forms Alliances with Bleu and Microsoft

Our infrastructure and ecosystem investments

Our solution is built on infrastructure that is in place in Europe today. Microsoft's foundational investments in datacenter infrastructure across Europe dates back nearly two decades.

Beginning in the early 2000s, the company started building its European datacenter footprint, which has since grown to over 200 facilities across 16 countries, contributing to a global network of more than 400 datacenters in 38 countries, all connected by 600,000+ kilometers of fiber. These purpose-built facilities support secure, high-availability digital services, including cloud computing, AI workloads, and data analytics. In response to rising demand, Microsoft announced plans to more than double its European datacenter capacity between 2023 and 2027.

Beyond our infrastructure investments, Microsoft actively partners with European cloud providers to deliver Microsoft applications and services on their local infrastructure. This includes the development of tailored technology and licensing solutions to support their specific market needs. As an example, Microsoft has entered into an agreement with the Cloud Infrastructure Services Providers in Europe (CISPE), the non-profit trade association for infrastructure-as-a-service providers in Europe, under which CISPE members may deploy Microsoft 365 Local on local European infrastructure if made generally available in Microsoft's Cloud Solution Program.

In addition, we have **National Partner Clouds**, operated by local partners to meet specific national requirements, such as France's Bleu and Germany's Delos Cloud. The National Partner Clouds are independently owned and operated clouds designed specifically to meet the national security and regulatory frameworks for public sector and critical infrastructure customers, and their use is restricted to those customers.

As we operate our own infrastructure and partner with others, in all cases Microsoft recognizes the importance of, and complies with, all applicable European laws.

Explore Microsoft's Global Datacenters

This document is intended for informational purposes only and does not constitute legal advice. Microsoft makes no warranties, express or implied, in or relating to this document. Customers remain responsible for their own risk assessments, mitigation measures, and which features and functionalities they choose to implement based on their unique context. For more detailed resources on Microsoft's comprehensive set of sovereign capabilities for productivity, security and cloud solutions in Europe, customers can refer to www.microsoft.com/sovereignty

Discover more at microsoft.com/sovereignty

Microsoft