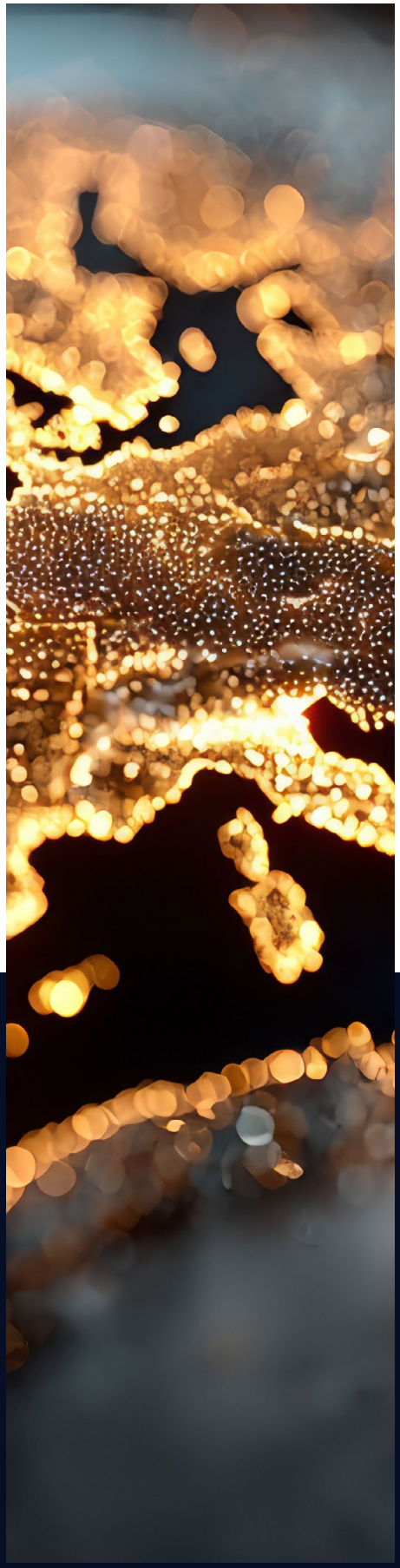
Private and Sovereign AI: Orchestrating control at scale for autonomy, resilience and advantage

Why NTT DATA is your end-to-end partner for secure, controlled AI

The rise of private and sovereign AI



For many organizations, AI strategy thus far has centered on scale, speed and model performance, based on the assumption that data could move freely and infrastructure could be global.

But these strategies are now being challenged by issues that are as much geopolitical and regulatory as they are technical: where data is stored, who controls the intelligence layer, what happens when jurisdictions diverge and how organizations protect sensitive intellectual property (IP) amid geopolitical tensions.

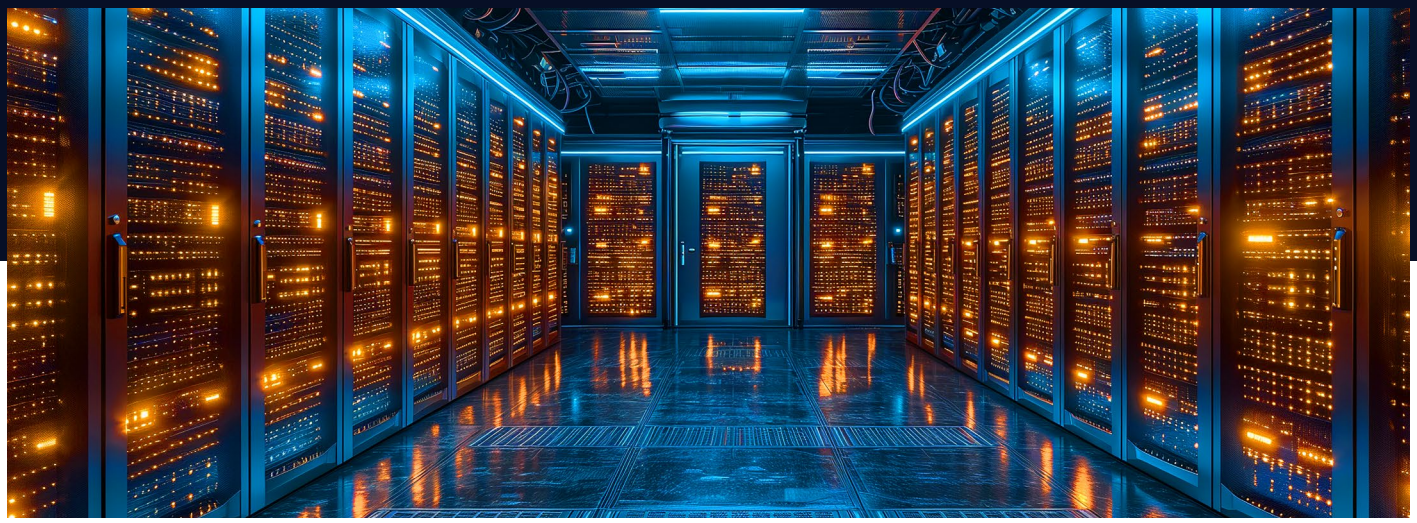
In this context, a shift to private and sovereign AI is becoming a strategic imperative. Forward-thinking organizations are already treating privacy and sovereignty as cornerstones of sustainable AI design and transformation.

Defining private and sovereign AI

Private AI refers to AI systems deployed within an organization's own controlled environment, such as private cloud or on-premises infrastructure, for data privacy, security and access control. Sovereign AI goes a step further by incorporating legal and geopolitical requirements: It ensures that data, infrastructure and AI operations remain subject to a specific jurisdiction's laws and governance frameworks.

New global NTT DATA research[1] confirms both the urgency of this evolution and the opportunities it creates. Almost all organizations (**95%**) say sovereign or private AI is important to their AI strategy, yet fewer than half (**47%**) have full confidence they can meet data sovereignty requirements. The challenge is clear: Organizations need AI to remain competitive, but they cannot compromise on data sovereignty, security or regulatory compliance.

[1] NTT DATA. 2026 Global AI Report: A Playbook for Private and Sovereign AI. May 2026.



Three powerful, interconnected forces are accelerating the shift toward private and sovereign AI:

01

Regulation

In highly regulated industries such as banking and healthcare, compliance requirements are intensifying. In Europe, for example, frameworks such as the General Data Protection Regulation, the NIS2 Directive, the Digital Operational Resilience Act (DORA) and the EU AI Act are raising the bar for how AI systems are deployed, governed and audited. This growing scrutiny is reflected in sentiment: **96%** of organizations fear privacy violations and misuse of customer data related to the use of AI and GenAI, and a most CEOs (**57%**) identify data privacy and sovereignty across geographies and environments as their foremost security or governance threat.

02

Geopolitical uncertainty

Rising global tensions are amplifying the need for assured control over data and AI infrastructure. For public-sector and defense organizations — where systems underpin national security, citizen data and public services — sovereignty is a mandate, not a choice. Accordingly, **96%** of organizations agree (**45%** strongly) that they are considering relocating AI infrastructure to specific geographies because of geopolitical pressures and concerns around supply chain provenance.

03

AI-driven requirements

Effective AI adoption depends on well-defined data boundaries, predictable processing environments and stringent access controls. At the executive level, this is widely recognized: **98%** of leaders consider it essential to establish private domains that safeguard IP and sensitive data.

As private and sovereign AI environments emerge as a foundation for competitive advantage, NTT DATA is helping organizations to design, implement, operate and manage these environments — turning compliance imperatives into competitive advantages, regulatory requirements into strategic assets and control into capability at scale, all within a unified AI estate.

From strategic priority to operational reality

Organizations that view private and sovereign AI purely through a compliance lens capture only a fraction of its potential. Sovereignty enables trusted AI deployment, faster innovation and sustainable competitive positioning. However, for many technology leaders, translating this ambition into operational reality remains a significant challenge.

The primary constraint on scaling AI is now infrastructure, not the models themselves. Nearly all organizations (**96%**) report that legacy infrastructure is actively slowing AI adoption, and more than half (**51%**) cite integration complexity in hybrid environments as a top concern when running AI workloads in private cloud environments. Among those advancing sovereign AI strategies for GenAI, **40%** identify infrastructure modernization as their single biggest challenge, compounded by the difficulty of assessing and integrating complementary technologies.

This complexity is amplified by industry-specific requirements:

- **Financial services:** Regulations such as DORA demand that institutions retain sufficient control to audit, modify or terminate critical AI arrangements without operational disruption — a standard that cloud deployments subject to foreign jurisdictions often struggle to meet.
- **Manufacturing, automotive and defense:** Sensitive IP and classified workloads must remain within enterprise boundaries, necessitating architectures designed for sovereignty from inception.
- **Critical infrastructure (energy, utilities and transportation):** Resilience and the ability to isolate systems and data are non-negotiable design imperatives.
- **Public sector and healthcare:** Sovereignty extends to ensuring states' operational continuity and healthcare providers' clinical governance, with mandates that determine architectural decisions rather than merely influence them.

Control over computing, data and AI models is fast becoming as strategically significant as capital, supply chains or human talent. Ultimately, a private or sovereign AI strategy is only as strong as an organization's capacity to execute it.

Balancing compliance, cost and control without compromise

Sovereignty should be understood not as a constraint but as a prerequisite for sustainable transformation. NTT DATA enables organizations to strike the right balance between compliance, cost and control at scale, through a comprehensive portfolio of solutions grounded in domain expertise, strategic autonomy and localized governance.

Addressing sovereignty from infrastructure to intelligence

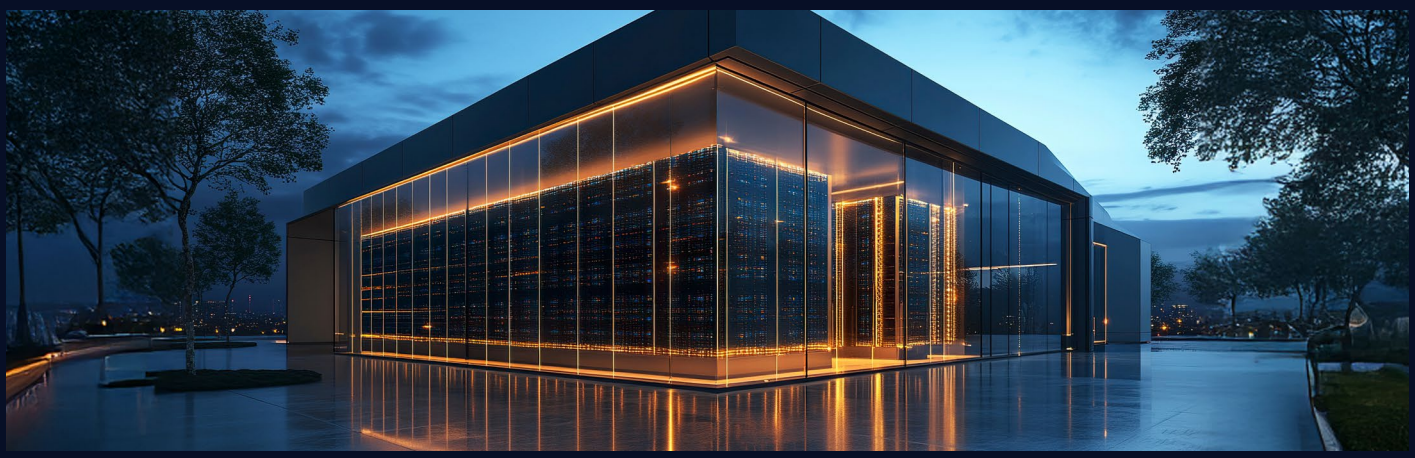
A full-stack approach is essential to achieving end-to-end control and resilience throughout the AI lifecycle, from physical data centers and AI infrastructure to platforms, models and security. This begins with our purpose-built data centers, designed to meet the power, cooling and network demands of AI. On this foundation, NTT DATA's Enterprise AI Factory and agentic enterprise tools establish environments optimized for AI workloads, with embedded accountability for performance, compliance and cost efficiency.

These capabilities extend across industries to support sensitive and domain-specific data needs: safeguarding patient and genomic data in healthcare, protecting proprietary actuarial models in insurance, securing creative IP in media and entertainment, and ensuring algorithmic integrity in financial services. In doing so, organizations gain strategic ownership of the AI assets that underpin long-term competitive advantage — computing, data and models.

Ecosystem orchestration and strategic partnerships for innovation at scale

We bring together best-of-breed, vendor-agnostic ecosystems grounded in long-standing partnerships with NVIDIA, Cisco, Dell, Mistral AI and hyperscalers such as Microsoft, Amazon Web Services and Google. These partnerships enable coordinated architecture design, ongoing performance optimization and access to innovation at every stage of the sovereign AI journey.

Our ecosystem orchestration model also reinforces strategic independence. Multiprovider architectures mitigate concentration risk and reduce organizations' reliance on any single supply chain — an increasingly critical requirement in regulated industries such as banking and the public sector, where operational resilience and risk diversification are mandated.



A hybrid approach balancing flexibility and control

Striking the right balance between control, agility and compliance is central to private and sovereign AI. With our help, organizations can design and implement hybrid architectures that blend public cloud with private and sovereign environments, allocating sensitive data and regulated workloads to controlled domains while using public cloud where risk is lower and economic efficiency matters.

This approach preserves sovereignty without limiting access to global AI innovation. Workloads are placed deliberately, aligned with regulatory requirements, strategic priorities and risk thresholds. In practice, this supports demanding, industry-specific needs such as protecting pharmaceutical R&D and clinical trial data or enabling explainable AI in financial services and insurance.

How NTT DATA's Private and Sovereign AI services support clients

Our comprehensive private and sovereign AI capabilities span the full lifecycle, from strategy to ongoing operations:

- **Strategy and economics:** Through global procurement networks and repeatable modernization playbooks, we help organizations adopt and scale AI securely and with confidence. Our experts pinpoint where AI can deliver the greatest business impact and develop structured roadmaps for responsible, enterprise-wide AI transformation, addressing every dimension of sovereignty.
- **Architecture advisory and sovereign AI assessment:** We map workloads in public, private, sovereign and AI-specific environments, supported by cost-versus-risk analyses to inform investment decisions. This process includes the identification of infrastructure limitations for private and sovereign approaches.
- **Security and governance:** We advise clients on AI security, privacy and compliance, including the design of control frameworks and governance models as well as necessary IT modernization actions.
- **Design and build:** We design sovereign AI architectures across environments end to end, using proven reference architectures and standardized landing zones customized to client requirements.
- **Ongoing operations and optimization:** Our clients benefit from continuous governance, compliance monitoring, cost optimization and the provision of audit-ready evidence to support regulatory requirements.

Industrializing AI with Enterprise AI Factory

Scaling AI from isolated pilot projects to enterprise-wide intelligence requires a proven, disciplined operating model, supported by expert assistance from the right partner.

Our **Enterprise AI Factory** unifies secure infrastructure, intelligence and operations, combining full-stack ownership with advanced optimization and proven delivery practices.

We industrialize the entire AI lifecycle — from data ingestion and model development to fine-tuning, deployment and high-volume inference — within a cohesive, production-grade framework.

The result is a streamlined path to designing, building and scaling AI systems, with stronger governance and less operational risk.

By integrating AI facilities, infrastructure, platforms and services with embedded governance, quality assurance and operational rigor, the Enterprise AI Factory converts AI ambition into sustained, measurable business outcomes. It establishes AI as a repeatable, scalable capability, which accelerates time to value, enables new revenue models and delivers defensible competitive differentiation.

The model is built on four tightly integrated layers — AI Services, AI Platform, AI Infrastructure and AI Facilities — and delivers precertified sovereign environments designed to reduce the high failure rates associated with AI pilot projects.

Organizations adopting this approach benefit from:

- **Lower total cost of ownership** driven by optimized AI infrastructure and operational efficiency
- **Faster progression from concept to production,** enabled by standardized, productized AI environments
- **Greater confidence in compliance and risk management**, including data residency and regulatory alignment

Turning an AI imperative into a competitive advantage

Global scale with local expertise

NTT DATA brings together more than 17,000 data and AI practitioners in over 70 countries, blending global experience with on-the-ground expertise to navigate local compliance and regional requirements. Through global procurement relationships, repeatable modernization playbooks and operational excellence, we help you move faster with AI, turning ideas into measurable business value while keeping complexity and risk in check. Our experts work alongside you to translate policy and control requirements into production-ready environments that scale with confidence.

Deep domain expertise across industries

With more than 35 years of experience in the public sector, healthcare, financial services, manufacturing and other industries, we apply our domain expertise to industry-specific data challenges. We go beyond broad compliance to meet the precise requirements of each regulatory framework, whether that's DORA and MiFID in financial services, clinical governance in healthcare, citizen data and national security obligations in the public sector, or OT integration in the manufacturing and automotive industries.

Strategic autonomy, control and localization

We build autonomy, control and localization into every architecture and partnership, turning sovereignty ambitions into practical designs, operational models and sustainable cost structures that enable you to command your AI future with confidence. We support you end to end — from strategy and design to build, deployment, operations and ongoing improvement.

Strategic independence and trusted partnerships

Independence matters in the private and sovereign AI era. Our broad partner ecosystem — spanning NVIDIA, Cisco, Dell, Hitachi and hyperscalers like Microsoft, AWS and Google — helps reduce supply chain risk and avoids dependence on any single provider. Our partnership with Mistral AI further expands access to European AI capabilities, giving you a genuinely vendor-agnostic foundation for sovereign AI across regions, jurisdictions and technology stacks.

Proven leadership in AI transformation

HFS

HFS Horizons Report | 2025

NTT DATA is recognized as a Leader in the HFS Horizons: Generative Enterprise™ Services 2025 report, highlighting its strong global presence and expertise.

Download the report

ISG

ISG Report | 2025

NTT DATA is named a Leader in the ISG Provider Lens® 2025 report for Agentic AI Services on a global scale.

Download the report

Everest Group®

Everest Group Report | 2025

NTT DATA named a Major Contender in the Everest Group Artificial Intelligence (AI) and Generative AI Services PEAK Matrix® Assessment 2025.

Read more

Gartner

Gartner Report | 2025

NTT DATA is recognized as a representative vendor in the Gartner® Market Guide for Generative AI Services for Banking (January 2025), highlighting its capabilities in the banking sector.

Read more

NTT DATA: Your end-to-end partner for sovereign, secure and controlled AI

As AI adoption accelerates and sovereignty requirements tighten, turning strategy intent into operational capability comes down to sound architecture choices, a clear operating model and the right partner.

Our industry experts bring deep advisory experience to help you navigate these decisions and design private and sovereign AI strategies around your regulatory obligations, risk profile and business goals. The challenge lies in the trade-offs: building environments that meet sovereignty requirements without adding unnecessary cost, operational friction or performance constraints.

We work with you end to end, designing, building and running sovereign AI environments that turn compliance imperatives into competitive advantages, regulatory requirements into strategic assets, and control into capability at scale. Our teams help you identify where AI can deliver the most value and map out a responsible path to enterprise-wide adoption that balances every dimension of sovereignty.

Our portfolio spans the needs of every industry, from regulatory demands in banking and healthcare to IP protection in manufacturing and automotive, and national resilience in the public sector — grounded in strategic autonomy, control and localization.

If you need both assured compliance and full control, along with the ability to use private and sovereign AI as a competitive edge, NTT DATA provides a trusted path to secure, scalable outcomes.

Visit nttdata.com to learn more.

NTT DATA is a $30+ billion business and technology services leader in AI and digital infrastructure. We accelerate client success and positively impact society through responsible innovation. As a Global Top Employer, we have experts in more than 70 countries. NTT DATA is part of NTT Group.

NTT DATA


NTT DATA