

Digital Sovereignty in the *Telco Sector*

Engineering the balance between sovereign
control and AI-driven growth



Microsoft



1 | Executive Summary

Digital sovereignty in telecommunications is no longer a specialist compliance topic. It is now a board-level growth issue because the same data, platforms and network functions that make telcos strategically important also make them difficult to modernize safely at scale. As operators pursue AI-enabled customer growth, autonomous networks and higher-value B2B services, sovereignty becomes the condition for using their most sensitive data and infrastructure with confidence rather than a brake on innovation.

That is why the right question is no longer whether a telco should be sovereign. The real question is where and how it should increase its sovereignty position across the estate, for maximum effect. Sovereignty is configurable, not binary. Different workloads require

different levels of jurisdictional assurance, operational control and technical protection. The objective is not to maximise control everywhere, but to apply the lowest-friction operating model that still satisfies regulatory, resilience and trust requirements.

This is where the joint Capgemini–Microsoft proposition matters. Microsoft provides a continuous sovereign architecture, spanning assured hyperscale, by-design public cloud, national partner clouds and sovereign-private deployments, all anchored in a common control framework (gated instances). That continuity matters because it lets an operator evolve its sovereignty posture without repeatedly re-platforming the estate. Capgemini offers guidance on optimal use of sovereign-related accelerators and services, translating architectural capability into working outcomes, regulation into workload decisions, integrating technology, governing the wider partner ecosystem, plus building and operating the end-to-end solution required to run and monetize sovereignty at scale.

The commercial implication is significant. Telcos increasingly seek to balance sovereignty, security, and innovation without unnecessary trade-offs. If sovereign controls are engineered correctly, operators can modernize customer and operational platforms, unlock generative AI on sensitive data, and create new revenue streams in sovereign B2B, public sector and industry markets. Without that capability, the operator is forced into a false trade-off: either accept elevated legal and operational exposure or constrain innovation in the very domains where growth is now expected.

This paper therefore addresses sovereignty in two connected ways:



1) Telco as a consumer of sovereign cloud: how operators modernize their own estate and unlock AI-led efficiency and growth under sovereign conditions.



2) Telco as a provider of sovereign cloud and AI: how operators can monetize sovereign infrastructure and trusted local operations as a differentiated market proposition.

The two are mutually reinforcing. Modernization builds internal sovereign capability and market credibility; monetization helps fund further modernization.

The conclusion is deliberately provocative.

In telecoms, sovereignty is not a defensive posture to be minimised. It is a strategic capability to be engineered: selectively where control matters most; consistently through a common control plane; and commercially where sovereign trust can be turned into enterprise value.

The Capgemini–Microsoft approach is designed to provide a structured path to turn digital sovereignty into measurable growth. It enables bold reinvention of the core business, supporting the development of new B2B revenue opportunities, expanding service portfolios, and monetizing technology and data assets, while modernizing through AI, cloud, and automation - helping Telco reduce operational complexity, support innovation at scale, and enable more differentiated customer experiences, depending on implementation. Crucially, it embeds security, regulation, and sustainability at the heart of transformation, positioning them as strategic advantages that accelerate resilient, trusted, and future-ready growth.





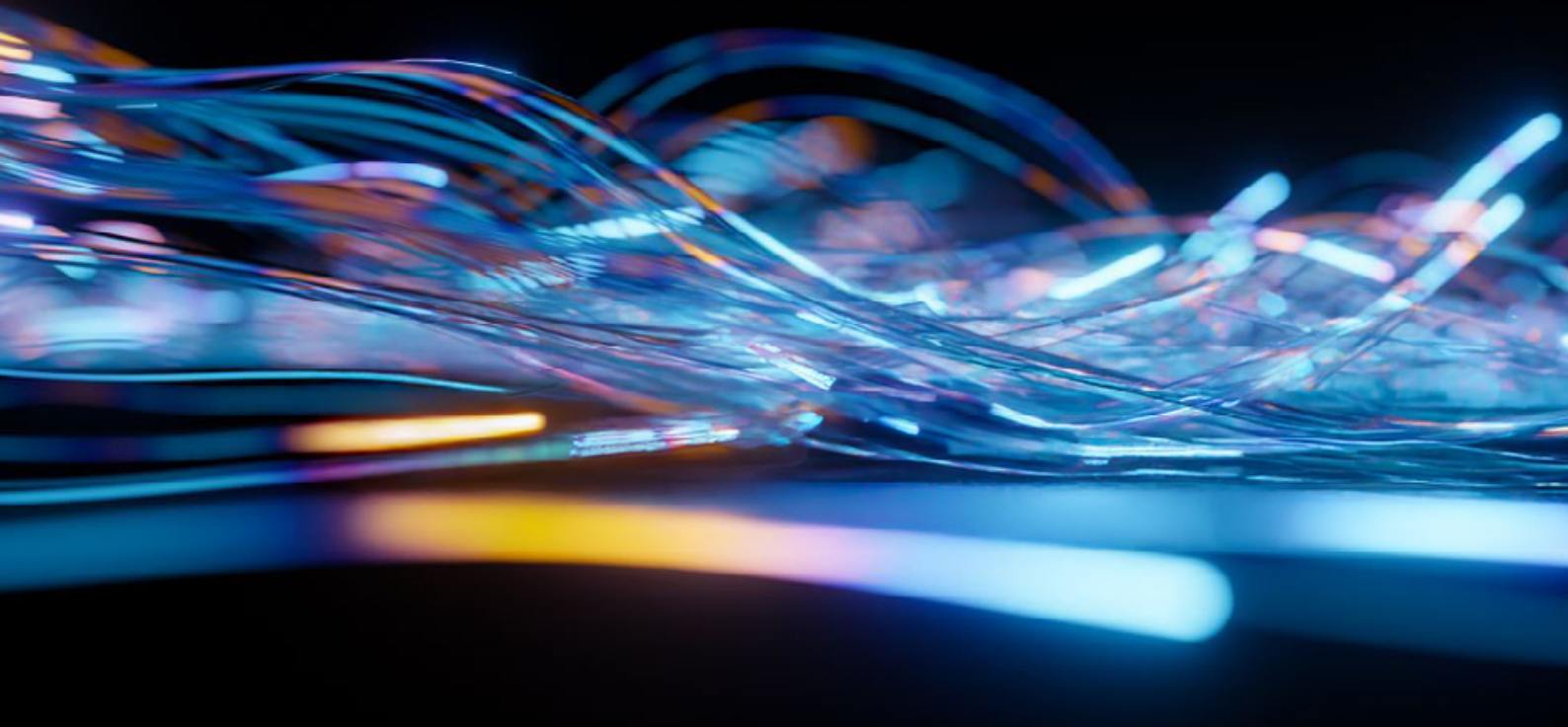
2 | Why Sovereignty Matters Now To The Telco Sector

Telecommunications operators sit at the intersection of critical national infrastructure, highly sensitive data, strict regulatory oversight and platform-disruption pressure. With growth ambitions across B2B and B2C, sovereignty is often a key requirement under regulatory and operational frameworks - it is embedded in licensing and public trust, and it applies with greater force than in almost any other sector because the telco is the substrate on which other sectors' sovereignty depends.

This creates a dual strategic reality. As consumers of sovereign capability, telcos must modernize networks, OSS/BSS, customer platforms and AI environments without breaching telecom-specific control requirements. As providers, they are increasingly well positioned to supply sovereign cloud and

sovereign AI services into markets that need trusted local infrastructure but cannot economically build it themselves. In other words, telcos are not simply subject to the sovereignty agenda; they are potential instruments of it.

A defensible posture must address overlapping regimes more complex than in most sectors, because telcos uniquely combine critical-infrastructure obligations, personal data, AI-enabled service delivery and national-security interfaces. GDPR and UK GDPR shape the treatment of subscriber and location data. Telecom-specific ePrivacy obligations and lawful-intercept requirements impose additional control expectations. NIS2, the EU Data Act and data portability requirements reshape resilience and exit expectations. The Cloud and AI Development Act (CAIDA), now in force, adds further



obligations around sovereign control of AI training data, inference transparency and critical AI infrastructure accountability. National telecom regulators and ETSI / 3GPP requirements further constrain network deployment models. Together, these pressures mean that sovereignty in telecoms is not a narrow cloud issue; it is a core operating model concern with direct ExCo relevance.

To reinforce, sovereignty is no longer a forward-looking consideration; it is an immediate strategic imperative, and the pace of change is accelerating faster than many operating plans assume. Four forces are converging. First, geopolitical fragmentation has turned jurisdiction into a strategic variable rather than a procurement detail. Second, 5G standalone, cloud-native network functions, edge and AI have increased dependence on a concentrated set of global technologies at the same moment as resilience expectations are rising. Third, subscriber metadata, location, billing and network telemetry have become more valuable in an AI economy and more exposed in a cyber one. Fourth, regulation across telecoms, data, resilience and AI increasingly demands auditable control over where data, operations and accountability sit and who can compel access.

There is also a broader policy shift underway. European sovereignty policy is moving beyond a narrow compliance lens toward a more explicit industrial agenda for cloud, AI, data centers and strategic digital capacity. For telcos, that matters because they are not only regulated entities inside this transition; they are also potential infrastructure providers within it. A credible sovereignty position therefore protects the license to operate while simultaneously opening a route to participate in the next wave of sovereign digital growth.

Against this backdrop, the cost of inaction compounds quickly. Operators risk deepening dependency and lock-in across the stack, exposure to supply-chain disruption, and rising regulatory exposure with both financial and operational consequences. In some cases, limited sovereign capability may affect trust and the ability to scale certain services. In an increasingly trust-driven economy, the absence of sovereignty is not merely a risk posture; it is a growth constraint.



3 | Capgemini's Position

Sovereignty is a spectrum, not a binary, and it is a transformation problem rather than a product problem. Operators should distribute workloads across levels of control and assurance according to sensitivity, legal exposure and resilience need; they should not apply maximum control uniformly. The practical objective is to engineer the right balance between trust, economics and innovation. Value may be created, not by pushing the whole estate to the highest possible level of isolation, but by matching each workload to the lowest control environment that still passes regulatory scrutiny, jurisdictional stress-testing and continuity requirements.

Sovereignty can be implemented within cloud architectures through a range of controls; it is workload-dependent. In practice, that means operators can use an architectural continuum and a common control plane while tightening or relaxing sovereign controls by workload rather than rebuilding the estate around isolated point solutions.

Capgemini's role is correspondingly specific – the translation of external drivers into architecture, architecture into an operating model, and operating model into business outcomes. That means defining workload placement, designing sovereign and hybrid patterns across IT, network and AI domains, integrating

Microsoft technology with the broader telco landscape, maximizing / operating run capabilities, and ensuring that sovereignty does not stop at compliance but becomes a means to modernize and monetize. The platform is Microsoft; the transformation discipline that makes it work within a telco is Capgemini.

Microsoft provides significant opportunities in addressing the digital sovereignty challenge. Azure and Microsoft 365 represent a robust and trusted foundation within the broader implementation landscape. However, the full scope of the challenge requires a wider set of capabilities. Telcos operate complex environments that include non-Microsoft applications, retail and customer operations platforms, and network technologies such as Open RAN. Capgemini's role is to provide impartial orchestration across this ecosystem: integrating the end-to-end solution while preserving client choice and flexibility. This paper highlights Microsoft technologies on their individual merits, without positioning them in comparison to other providers.

A strategic sovereignty posture should be engineered where it generates trust, regulatory viability and growth, not expended indiscriminately where it does not.

4 | Digital Sovereignty Across the Value Chain

Sovereignty spans the whole digital value chain, not just cloud and data. It is the capability to be resilient, to retain strategic autonomy, to reduce exposure to foreign interference end-to-end, and to maximize corporate potential. In many cases, full sovereignty

across every domain may not be necessary; the goal is to calibrate the appropriate level of control across cloud, connectivity, cyber, software, hardware and skills without constraining innovation and growth.

For this partnership, the paper focuses on



Within cloud specifically, Capgemini assesses sovereignty across five dimensions.

Dimension	Description
Operational Sovereignty	Assesses whether the operator controls who can operate and access the technology that delivers the service.
Data Sovereignty	Evaluates whether the operator controls where data resides and can trust who manages it.
Technical Sovereignty	Examines whether the end-to-end supply chain can be trusted.
Legal Sovereignty	Determines whether the organization has appropriate jurisdictional control and legal capability, with exposure to extraterritorial reach reduced to a level consistent with risk appetite and regulatory requirements.
Skills and Capability Sovereignty	Tests whether in-jurisdiction skills exist to run and sustain the service over time.

This broader framing matters because the most common mistake in sovereignty programs is to equate residency with sovereignty. Residency is necessary, but not sufficient. A telco also needs operational traceability, access governance, legal defensibility, resilient skills and, increasingly, portable architectures that preserve optionality under changing geopolitical or regulatory conditions.

The value this unlocks is not merely defensive. Sovereign capability lets operators scale AI on their most valuable and sensitive data, meet regulatory and trust expectations, and evolve beyond connectivity into sovereign AI and platform players. That creates a foothold in markets where demand for trusted, compliant and locally governed solutions is increasing, translating sovereignty from a control requirement into a lever for growth and long-term value.

Modernization generates opportunity for monetization; enabling future growth and corporate success.

While Capgemini uses these five dimensions as a practical operator-focused framework for assessing sovereignty across cloud transformation programs, they do not replace broader policy and assurance models. The following section aligns this practical lens to the European Commission's SEAL framework, which expands sovereignty across eight dimensions and five assurance levels. Together, they provide a structured way for telco operators to translate strategic sovereignty requirements into practical workload, operating-model, and investment decisions.

5 | The Sovereignty Spectrum

Sovereignty is not a binary choice between 'sovereign' and 'non-sovereign'. In line with the EU Commission definition, sovereignty exists in eight dimensions and sovereignty is a spectrum for each of those dimensions – there is never a binary state of not sovereign or full sovereign. Levels are then used to make the

spectrum usable. The spectrum is shaped by regulatory obligations, national resilience requirements, cybersecurity, risk, operational independence, commercial ambition and the pace of innovation. The issue is not simply where workloads run, but how the required control and autonomy is achieved.

This matters in both steady-state and disruption scenarios. An operating model that appears acceptable in normal market conditions may prove insufficient when tested by geopolitical tension, supply-chain disruption, legal compulsion and hostile activity, all of which may drive a need for accelerated recovery and re-platforming of critical services. In that context, sovereignty should be treated as a forward-looking design principle that is intended to support optionality, resilience, and risk mitigation - not just a compliance exercise.

In practical terms, the cloud sovereignty spectrum runs from low control / autonomy states through to high control / autonomy states. Between these poles sits a range of hybrid patterns: hyperscale services with enhanced controls, segregated landing zones, domestically operated environments, sovereign partner clouds and private cloud deployments for the most sensitive workloads. For most telcos, the end-state will not be a single architecture, but a deliberately layered model in which different workloads are placed according to their risk, criticality and regulatory profile.

This is why sovereignty decision-making should be evidence-based, incremental and investment-aware. The relevant executive questions are straightforward: what level of exposure is acceptable; what is the probability and business impact of loss of control; which data sets, platforms and operations present risk; and where does additional spend materially reduce strategic, operational or regulatory risk? In practice, customer data, lawful intercept, core network functions and nationally sensitive operational systems will typically justify a materially higher sovereignty threshold than more generic enterprise workloads.

The European Commission's SEAL model provides a useful structure for Digital Sovereignty because it recognises that sovereignty is multidimensional and progressive rather than absolute. It defines eight dimensions and five assurance levels, giving organizations a practical way to align workload placement and control requirements to a clear sovereignty ambition.

The eight sovereignty dimensions (SOV-1 to SOV-8) are:

Dimension ID	Name	Description
SOV-1	Strategic Sovereignty	Ownership, governance, financing, value creation, and alignment to European strategic priorities.
SOV-2	Legal and Jurisdictional Sovereignty	Exposure to non-EU law, external legal compulsion, and the jurisdiction in which rights and intellectual property are anchored.
SOV-3	Data and AI Sovereignty	Control of data location, encryption, access, deletion, processing, and AI governance.
SOV-4	Operational Sovereignty	The degree to which trusted in-region actors can operate, support, migrate, and sustain services independently.
SOV-5	Supply Chain Sovereignty	Provenance and auditability of hardware, firmware, software, and subcontracted dependencies.
SOV-6	Technology Sovereignty	Openness, interoperability, standards alignment, portability, and freedom from intractable lock-in.
SOV-7	Security and Compliance Sovereignty	Certifications, audit rights, security operations, patching authority, and control effectiveness.
SOV-8	Environmental Sustainability	Energy efficiency, circularity, emissions transparency, and resilience of energy sourcing.



The five assurance levels create a practical maturity scale:

SEAL Level	Name	Description
SEAL-0	No Sovereignty	Technology, service and operations remain under exclusive non-EU control.
SEAL-1	Jurisdictional Sovereignty	EU law formally applies, but practical control remains limited and non-EU influence is still dominant.
SEAL-2	Data Sovereignty	EU law is enforceable and data protections are strengthened, but material non-EU dependencies remain.
SEAL-3	Meaningful EU Control / Digital Resilience	EU actors have meaningful influence and non-EU control is marginal, supporting stronger resilience outcomes.
SEAL-4	Full Digital Sovereignty	Technology, operations and critical dependencies are fully controlled within EU jurisdiction.



Mobilizing the spectrum

Capgemini will support Telco operators with the spectrum considerations; reviewing, assessing and defining the capabilities required for success - acting as trusted partners and bringing industry experience and deep-rooted skills at every stage.

Microsoft technologies can help telco operators raise assurance in a controlled and modular way, showing alignment to SEAL levels. The value proposition is not that one control delivers sovereignty in isolation, but that a coherent control plane, spanning identity, policy, governance, encryption, monitoring and access transparency, allows an operator to enforce consistent standards across a multi-environment estate while retaining a common compliance and assurance function.

At the estate level, capabilities such as the EU Data Boundary, Advanced Data Residency and Sovereign Landing Zones can provide stronger residency, segmentation and policy enforcement (note: public cloud typically aligns with SEAL 2 requirements). These are relevant for establishing a baseline of jurisdictional assurance and operational separation across management groups, subscriptions and workload domains.

For higher sensitivity use cases, additional controls can be applied in layers - customer-managed keys, supported by Managed HSM, strengthen independence over data-at-rest / in transit / encryption protections; confidential computing extends protection to data-in-use for selected high-assurance workloads; operational sovereignty features for restricted access workflows and enhanced operational transparency. Where a telco's sovereignty target extends to the highest assurance outcomes, sovereign partner cloud models and operator-controlled private cloud patterns may be required for the most sensitive systems and data.

The implication for telecommunications providers is clear: sovereignty should be engineered as a portfolio decision. The optimal model is likely to combine hyperscale innovation for suitable workloads, enhanced sovereign controls for regulated domains, and highly assured operating environments for assets that are nationally sensitive or mission critical. This is the practical path to balancing resilience, regulatory confidence, speed of innovation and economic efficiency.



6 | Microsoft Sovereign Cloud for Telco

Microsoft's strength is not a single product; it is a continuous architecture designed to support operational implementation of sovereignty requirements: the operator can tighten or relax the sovereign position of specific workloads without rebuilding the estate around disconnected platforms.

For telcos, that architecture maps cleanly to three deployment patterns. Sovereign Public Cloud supports by-design workloads in public cloud using enforceable controls. National Partner Clouds* address country-specific regulated environments where a standard region is insufficient; Bleu is a live proof point of this model and demonstrates that Capgemini and Microsoft

can jointly operationalize sovereign cloud at production scale. Sovereign Private Cloud addresses hybrid, edge and disconnected environments, especially where national control, operational isolation or degraded-connectivity resilience is required.

**National Partner Clouds: A cloud environment that runs Microsoft Azure and Microsoft 365 services, but is operated by a local, in-country partner; designed for organizations that need: data to remain under local legal jurisdiction / infrastructure controlled domestically / protection from foreign government access / compliance with national security or regulatory standards.*

A continuous sovereign architecture

Microsoft offers consistent architecture (gated instances) spanning standard Azure, the EU Data Boundary, Sovereign Public Cloud, Sovereign Private Cloud and National Partner Clouds, extending to

operator-owned, disconnected deployments on Azure Local. Because it is a common architecture (gated), an operator can raise or relax its sovereignty posture per workload, and over time, without re-platforming.

Microsoft sovereign layer	Telco use
Sovereign Public Cloud	By-design workloads: Sensitive OSS/BSS, analytics, subscriber AI.
Sovereign Private Cloud	Core network, edge and disconnected critical operations on Azure Local.
National Partner Clouds	Country-specific regulated sovereignty: Bleu (Orange–Capgemini) for France’s ANSSI SecNumCloud context; Delos Cloud (SAP subsidiary) for Germany’s BSI requirements.

Common control plane architecture across every tier

The Identity and access management model (including Microsoft Entra ID) provides a consistent approach to sovereign capable identity management for each platform, allowing the operator to control who can reach what across public, private and national sovereign environments. Azure Local also supports alternative authentication models and it is expected that this will expand in the future

Data governance (including Microsoft Purview) enables classification, lineage and policy enforcement so that data-tiering decisions become auditable and consistent across sovereign and hyperscale estates.

Infrastructure and Policy as Code (including Azure Arc) and policy-driven management-group structures provide management and compliance capabilities across cloud, sovereign-private and on-premises footprints. In practical terms, this means a common compliance and audit function rather than multiple parallel ones.

Architecture and designs should follow best practice and consider continuity requirements across the Microsoft technology stack, plus other capabilities such as multi-cloud, as required by client needs .

Sovereign AI — Microsoft Foundry (formerly Azure AI Foundry)

Microsoft Foundry adds a sovereign-capable, multi-model AI platform with regional control over model hosting, training-data isolation and inference logging. By supporting a broad ecosystem of models behind a consistent control plane, it is designed to help reduce potential dependency on specific AI supply chains and allows operators to respond to regulatory, geopolitical or trust-driven shifts without re-architecting every application. Microsoft Foundry Local extends this pattern into disconnected sovereign environments as product maturity allows.

Sovereign technical controls

The architecture is operationalized through a defined set of controls, some available today and some on Microsoft's published roadmap.

Sovereign Landing Zones provide the reference architecture and policy framework for operationalizing sovereign controls in Azure. Built on Azure Landing

Zones, they use management-group hierarchy, Infrastructure-as-Code, policy enforcement and reusable control libraries to turn sovereign intent into repeatable deployment patterns.

Data Guardian is a forthcoming Microsoft capability intended to add European-personnel oversight of privileged operational access, with approvals, monitoring and tamper-evident logging applied to sensitive operational access. This is relevant because sovereignty is not only about where data sits, but who can touch the systems that process it and under what audit conditions.

Customer-managed keys via Azure Key Vault Managed HSM provide a strong baseline approach for key custody. External Key Management is an emerging Microsoft capability that further strengthens independence by allowing keys to be held outside the provider environment. Regulated Environment Management is a forthcoming capability intended to simplify the configuration of sovereign controls.

Azure Confidential Computing protects data in use through hardware-based trusted execution environments, enabling sensitive workloads to process data while remaining encrypted in memory and designed to restrict access by unauthorized processes under defined configurations. Remote attestation provides additional assurance that the intended secure runtime is in place before execution.



Legal accountability and access governance

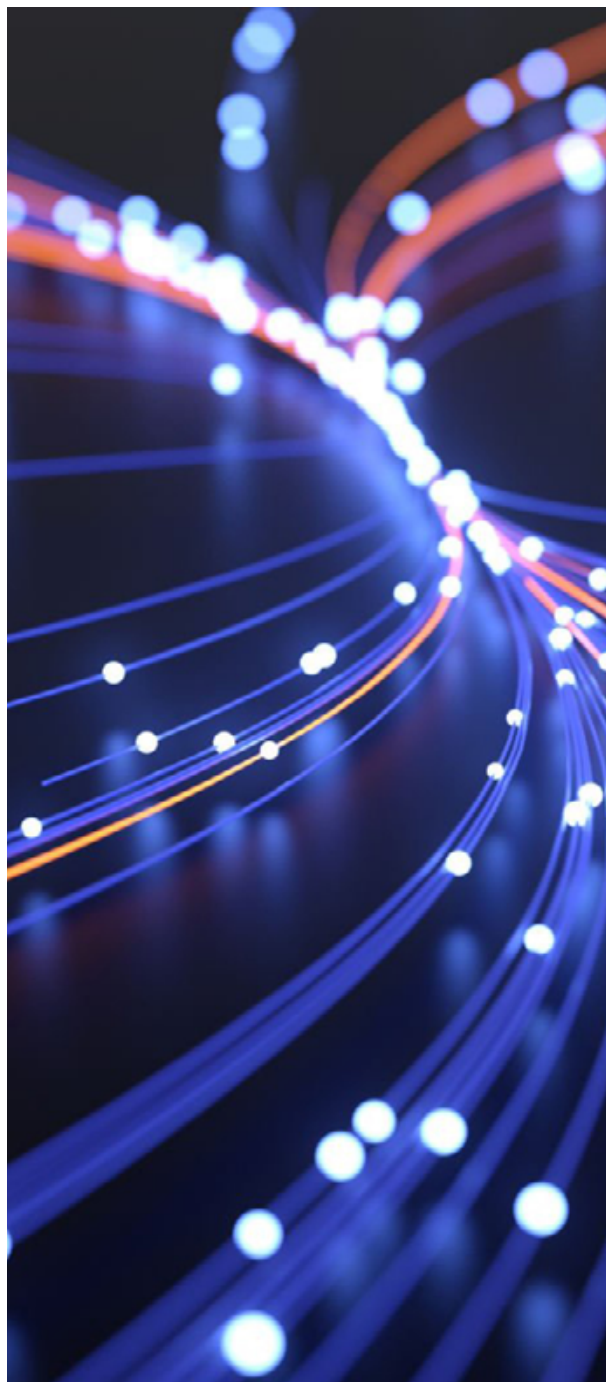
Sovereignty is also a legal posture, not only a technical one. Microsoft states that it does not provide direct or unfettered government access to customer data and reviews requests in line with applicable legal processes.

EU Data Boundary

Microsoft commits that customer data for core Azure, Microsoft 365 and Dynamics 365 services (including service-generated telemetry, logs and Copilot prompts and responses, though not billing data) can be stored and processed within the EU boundary. For assured-hyperscale workloads, this remains a cornerstone control for data residency and jurisdictional assurance, especially where telcos need to demonstrate that sensitive customer or operational data is not processed outside the intended region.

Azure Local - the carrier-grade hybrid platform

In support of operator-provided 5G core and network functions, Azure Local provides a carrier-grade managed hybrid platform in which the most sensitive control and user plane elements can remain under national jurisdiction while still benefiting from consistent governance and lifecycle control. These controls are one tier within a wider sovereignty architecture rather than the center of the whole story. For clarity, Microsoft is providing the platform (Azure / Azure Local) plus the control plane and AI. The network functions are supplied by the operator (or operator partners).



7 | Reversibility and Exit

A sovereignty position is not credible without an exit position. Sovereignty includes the freedom to leave — not as an abstract right, but as an engineered capability. The EU Data Act's switching and portability obligations reinforce this, but for telcos the underlying strategic issue is broader: if the operator cannot move the workload, move the data, or revoke operational dependency, it has not fully controlled its sovereign posture.

Portability by design therefore matters. Open, containerized and standards-based patterns should be explored, in line with other portability trade-offs, so workloads can be re-hosted with lower friction. This is especially important in cloud-native network functions, OSS/BSS integration layers and AI platforms, where dependence can otherwise accumulate invisibly over time.

Data and key custody are equally important. Customer-managed keys and Managed HSM provide strong present-day control over decryption authority, while External Key Management is expected to strengthen that control further as it rolls out. In the AI domain, model portability and decoupling between the AI platform and underlying models matter just as much; the goal is to avoid replacing one form of cloud lock-in with another form of model lock-in.

This is also where Capgemini's independence matters. The orchestration layer keeps options open and engineers reversibility, even where the implementation layer uses a single partner's technology. In sovereignty, exit architecture is not a legal appendix; it is part of the design.



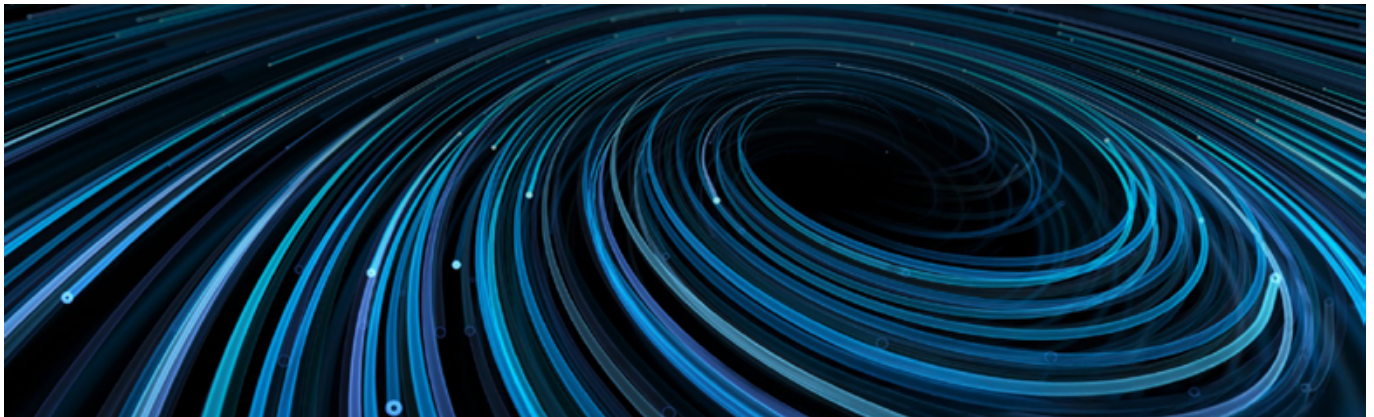


8

Telco as a Consumer

Sovereignty as a business-efficiency and growth agenda — a CTO/CIO decision about how to run the operator’s own estate more securely, more credibly and, over time, more profitably. The scenarios below show how telcos

move from objective to operating reality by linking business outcome, sovereignty requirement, Microsoft implementation pattern and Capgemini delivery.



Scenario 1 — Low complexity

A Tier 1 European operator migrates its legacy customer estate — CRM, digital self-service and customer-experience AI to cloud. The platform serves roughly 20 million subscribers and 150 million interactions a year, and the operator wants generative AI for service automation. The workload contains no core-network or lawful-intercept functions.

Tiering decision. The workload is deployed on Azure using a by-design approach inside an assured-hyperscale pattern, where controls are explicitly configured rather than assumed. The EU Data Boundary is deliberately enabled to support EU-only data residency and processing, reducing jurisdictional exposure. A Sovereign Landing Zone establishes the policy envelope and management-group structure. Microsoft Foundry provides a

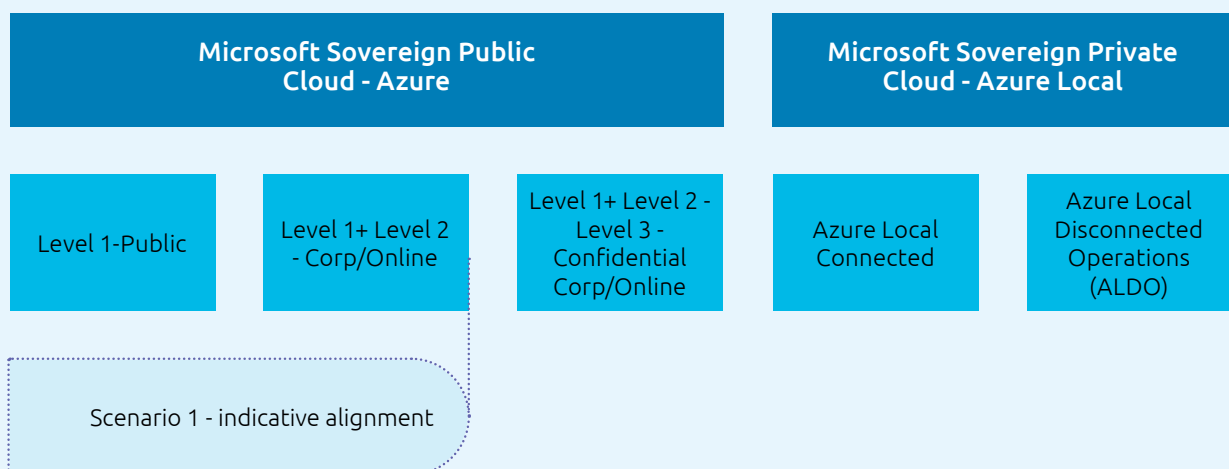
sovereign-capable, multi-model AI platform so the operator can adopt or change models without re-architecting the application stack. Customer-managed keys - optionally backed by Managed HSM - strengthen data control today, while Microsoft's forthcoming Data Guardian capability is expected to add European-personnel oversight of privileged operational access, with approvals and tamper-evident logging. External Key Management, also on Microsoft's roadmap, further strengthens key custody as it becomes available.

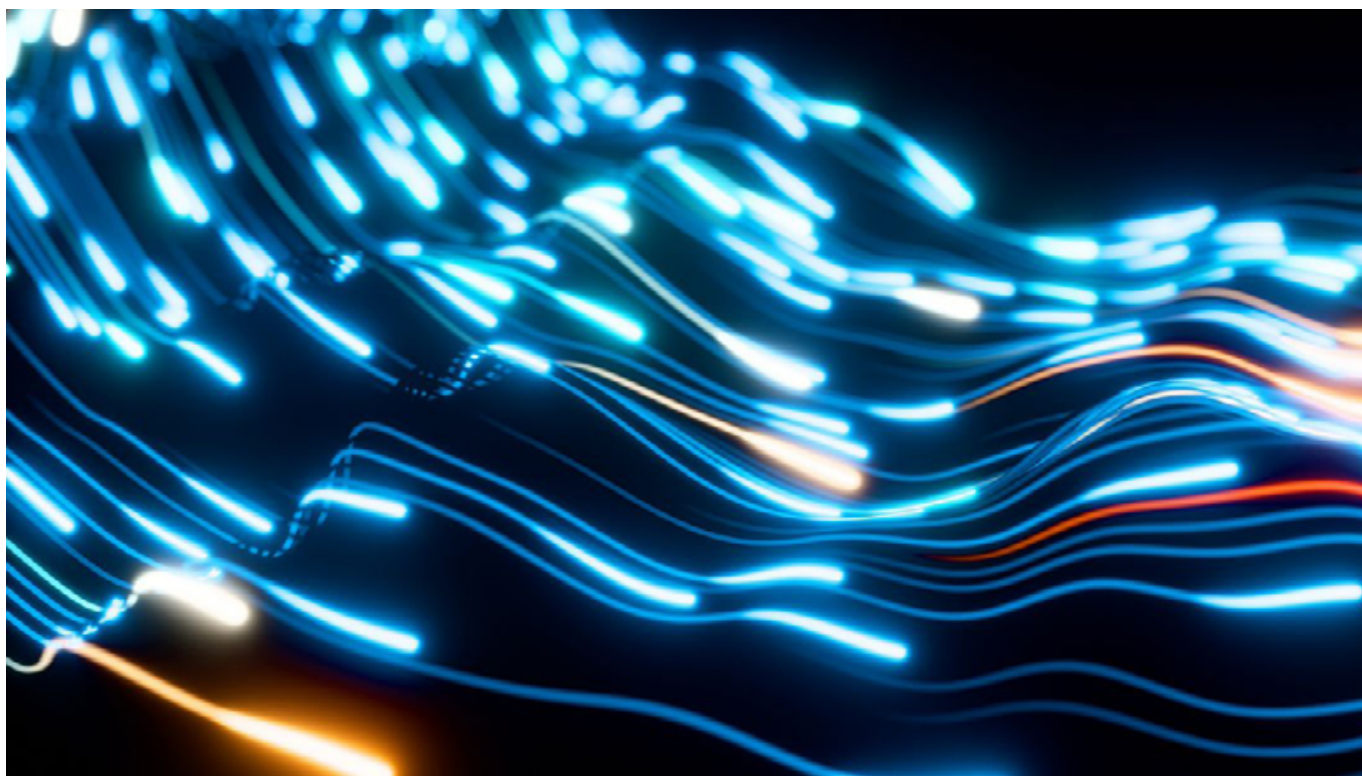
Indicative economics. Payback timelines may vary; in some illustrative scenarios, timelines of approximately 18 months have been observed based on specific assumptions. For this scenario, appropriate deployment and usage of solutions may contribute to reduced legacy-platform maintenance overheads (at steady state) and contact-center call volumes (at full AI deployment). The sovereign overlay sits at the low end of the premium curve.

What it proves. A well-segmented architecture supports the use of generative AI on subscriber data at scale, subject to appropriate governance and controls, without placing that data outside the intended jurisdictional boundary. The premium is not a surcharge on innovation; it is the cost of making AI on data legally and operationally viable.

Capgemini defines the workload placement, designs the landing zone and control pattern, integrates the new sovereign platform into the existing customer estate, and manages the broader ecosystem - including retail, customer-service operations, marketing or an incumbent non-Dynamics CRM.

Microsoft provides the AI and cloud foundation; Capgemini makes the operator's target state real.





Scenario 2 — Medium complexity

A major operator consolidates four legacy OSS/ BSS platforms — network inventory, service assurance, billing and workforce management — onto a single target. The programme covers roughly 8,000 internal users and 200+ network integrations. This is a larger, more complex and interconnected set of systems with components that have distributed location demands and sovereignty requirements.

Tiering decision. The solution adopts a deliberately layered hybrid architecture, segmenting workloads by sovereignty need. Billing and subscriber management run in a

by-design model using Microsoft Sovereign Cloud controls, with Sovereign Landing Zones, customer-managed encryption, operational access restrictions and in-jurisdiction oversight.

- The stateless front ends providing publicly accessible information sit in the public layer, and only subject to the location controls that are applied to the whole estate.
- The core system data requires stronger sovereignty and is encrypted at rest with customer-managed keys. These workloads are placed under the Corp and Online management groups and inherit stronger

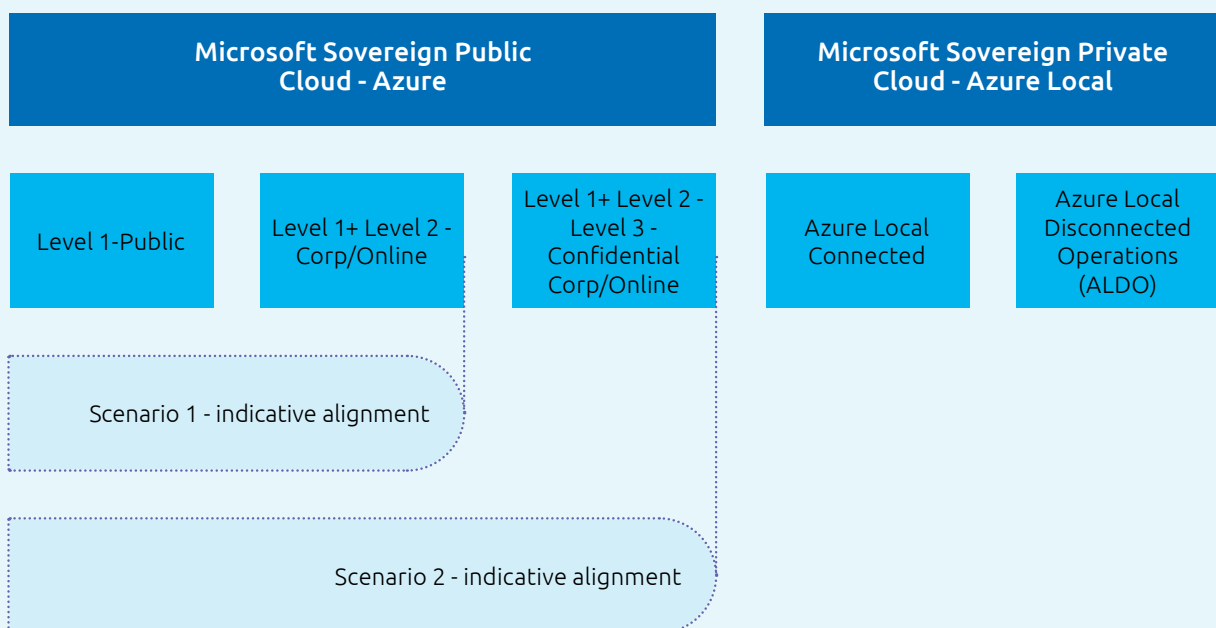
policy controls. The operator has full control over the HSM, creating the security domain and managing local RBAC. Therefore Microsoft is incapable of unilaterally accessing the keys and decrypting the data.

- The most sensitive systems - handling billing data and end-customer PII information – are additionally encrypted in use on a Confidential Compute platform.
- The integrations require workloads to be running in other data centers and these are onboarded as custom locations using Azure Arc, enabling a common plane for management, monitoring and compliancy reporting. Operational sovereignty capabilities include Data Guardian, Customer Lockbox and Transparent Logs. These could be running on Azure Local, but Azure Arc is flexible in supporting workloads hosted on other platforms, on-premises and multi cloud.

Indicative economics. Avoided cost comes from retiring four legacy stacks, while faster service and product configuration enables earlier enterprise launches. The blended premium sits in the middle of the sovereign-cost curve.

What it proves. The hardest challenge is not introducing sovereign controls into one workload; it is maintaining consistent identity, policy, audit and operational governance across more than 200 integrations without creating two parallel compliance functions. This is where the Microsoft control plane materially reduces complexity.

Capgemini translates regulatory expectations into architecture, defines the cross-tier identity and audit model, integrates the operator's retained systems, and establishes the operating model that allows the hybrid estate to run as one. This is the practical bridge between platform capability and business outcome.





Scenario 3 — High complexity

A multinational group operates in several European markets under a shared services and platform strategy. It must deploy cloud-native 5G standalone cores while satisfying conflicting national requirements: each regulator demands that its 5G core and lawful-intercept platform operate under that country's jurisdiction, even as the group wants common tooling, shared network analytics and a single operating model. A leader-follower deployment — one market proving the pattern and others adopting it — must not create cross-border data flows that breach any single jurisdiction.

Tiering decision. The decision is underpinned by the following principle - Microsoft is providing the platform (Azure / Azure Local) plus the control plane and AI. The network functions are supplied by the operator (or operator partners).

In each market, the 5G core functions and lawful-intercept platform run Azure Local under that country's jurisdiction. A few highly sensitive systems are hosted on isolated systems within country in Disconnected Operations mode,

with the control plane running directly on the cluster for completely local control and validated lifecycle management. The operator has adopted a default sovereignty stance of Connected mode for the remaining systems in order to benefit from centralized application deployment, management, governance and observability. Group-level network analytics and AI operations run in Microsoft Sovereign Cloud with per-market residency and no cross-border egress of regulated data. The operator needs the ability to strengthen their sovereignty posture in response to unexpected and unwanted events, and each location is configured to allow these systems to transition to Disconnected Operations should the need arise.

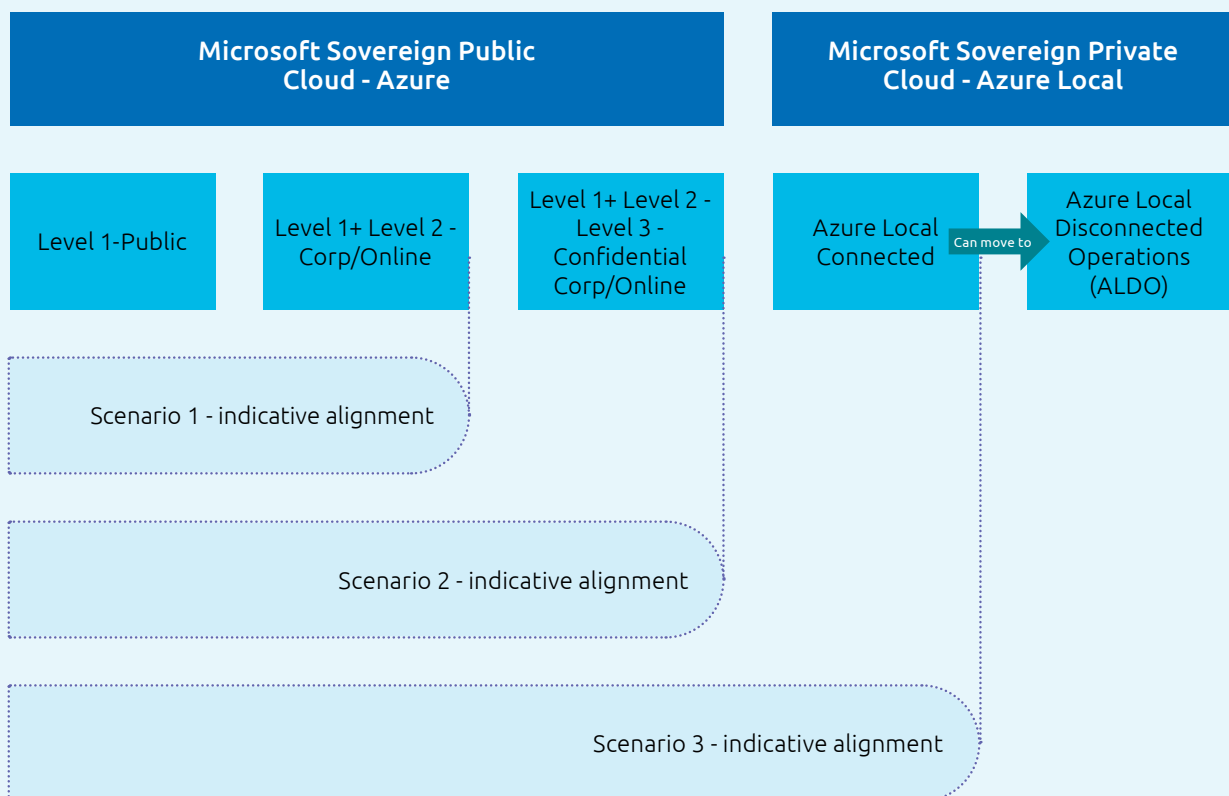
Why this scenario defines the market. This is the case many European groups increasingly face as 5G standalone accelerates. The tension is not country versus cloud, but country versus country versus group. The differentiator is an architecture that preserves shared

economics and a common operating model while demonstrating that each market's most sensitive functions remain within the required sovereign perimeter.

Indicative economics. The primary benefit is regulatory viability and continuity of license, combined with long-run value from a reusable multi-country operating model. This model is the top of the premium curve, offset by shared tooling and policy.

Capgemini orchestrates the transformation across markets and vendors, including integration with wider network ecosystems and open architectures where telcos are pursuing Open RAN and multi-vendor disaggregation.

Microsoft supplies the platform and control-plane components; Capgemini designs the cross-jurisdiction operating model and preserves architectural openness.





9 | Telco as a Provider of Sovereign Cloud

The commercial extension - Once operators have built credible sovereign capability inside their own estate, they gain the right to monetize that capability externally. Modernization and monetization therefore form a reinforcing loop: operators that use sovereign technologies themselves build the technical, regulatory and market credibility needed to sell sovereign services to enterprise and public-sector customers.

The opportunity is becoming clearer. Operators hold expensive, highly secure, nationally sovereign facilities and want to derive more value from them. At the same time, many markets will not justify a full sovereign

public-cloud region, yet still contain organizations that need stronger local control than standard public cloud can provide. This leaves a gap that a telco can fill by becoming a sovereign cloud and sovereign AI provider in its national market.

This is a core growth play, not a side experiment. Demand for trusted local cloud, AI and data services is increasing across regulated industries and government-adjacent markets, while national policy direction is placing more value on domestically governed digital capacity. Telcos already own the trust, locations, operational rigor and sector access that make this proposition credible.

How it works

The operator provides the sovereign-certified data centres and local operating environment; with Capgemini supplying deep expertise, industry insight and technical capabilities across the end-to-end activity. Microsoft provides the sovereign technology stack, including Azure Local for sovereign-private cloud patterns and the wider control-plane services needed for identity, policy, governance and AI. As product maturity and market need allow, local service portfolios can extend beyond infrastructure to collaboration, AI and developer services. The operator's customers then consume appropriately configured capabilities aligned with hyperscale cloud approaches, under national jurisdiction without having to build or operate it themselves.

Why it is complementary, not competitive

The operator is not competing with hyperscale economics at global scale. It is serving a segment that needs more sovereignty than standard public cloud can credibly provide in-country, but lacks the scale or appetite to build a sovereign platform independently. In that sense, the proposition is complementary: it extends sovereign digital capacity into places and sectors where direct hyperscale investment may be uneconomic or insufficiently localized.



The economics — affordability through aggregation

A dedicated sovereign-private platform is a substantial capital commitment that many small and medium organizations cannot justify. The Telco buys once, invests in the capacity and provides the sovereign capabilities of Azure Local across many customers - this can enable a transition toward a consumption-based service model. Additional value is created by providing many 'overhead' requirements as part of the overall service; accreditation, operations, lifecycle management, sovereign data hosting, managed AI services and local support can be included as aggregated services. The result is an affordability-through-aggregation model viewed from the provider's P&L rather than the consumer's cost base.

Key note - the exact nature of the consumable service (pay-as-you-go / fixed price etc) will depend on many factors such as the technologies involved and the consumer / provider appetite – this will need to form a key telco decision point. Capgemini can support throughout this critical decision process.

Three delivery options

Aggregated sovereign-private is the smaller, faster play: the operator hosts Azure Local-backed sovereign capacity and offers it as a service to SMEs, critical suppliers and regulated organizations.

A managed-service provider model for Sovereign Public Cloud is a lower-capital, services-led variant: the operator provides managed sovereign controls, onboarding, run services and support around public-cloud sovereign environments for enterprise clients.

The larger strategic play is the national partner cloud model, exemplified by Bleu, where sovereign cloud is delivered through a dedicated in-country structure aligned to specific national requirements.

The right model depends on market size, regulation, sovereign demand and investment appetite. The success of the model is enabled with Capgemini and Microsoft.

Operating model and resilience

The proposition should be operated by security-cleared, domestically based personnel, with privileged access controls, auditable assurance artifacts and clear shared-responsibility boundaries. Because sovereignty varies by industry and regime, the operator must articulate a tiered catalog aligned to different combinations of control and assurance. Connected and disconnected operating modes may both be relevant, particularly where local resilience and continuity under degraded connectivity conditions are part of the value proposition.

A worked example — national operator launches sovereign cloud-as-a-service

A national operator in a mid-sized European market with no dedicated sovereign hyperscale region stands up an Azure Local platform in its own certified facility and offers tiered sovereign capacity to regulated SMEs and public-sector bodies. Customers consume sovereign landing zones, infrastructure, platform services and — over time — sovereign AI services without the capital commitment of a dedicated platform. The operator absorbs hosting, accreditation, patching and lifecycle, and wraps it in a managed service.

Roles. Microsoft provides the platform and control architecture. Capgemini designs the service catalog, sovereign landing zones, customer onboarding and operating model, then helps the operator translate the technical platform into a saleable, supportable sovereign proposition.

Indicative economics. The operator converts a single capital commitment into recurring per-customer revenue, with additional margin from the managed-service wrap and potential expansion into sovereign AI or collaboration services as demand matures.

What it proves. A telco can monetize sovereign capability in a market the hyperscaler will not serve directly at full sovereign depth, turning sovereignty from an obligation into a new revenue line.





10

Capgemini's Differentiated Role

Many consultancies can define a sovereignty strategy; Capgemini's differentiation is the ability to orchestrate digital sovereignty as an end-to-end transformation across all domains, cloud models and business layers — and to run it. Sovereignty is not a product challenge. It is a change program that requires regulation to be translated into architecture, architecture into engineering, engineering into operations and operations into measurable business outcomes.

That translation role is especially important in telecoms because the estate runs across network, OSS/BSS, customer platforms, AI, cyber and operations, with multiple incumbent technologies and suppliers at every layer. Capgemini defines workload placement across sovereign, hybrid and multi-cloud environments; integrates Microsoft technology with the wider telco ecosystem; designs the controls and DevSecOps patterns required for sovereign execution; and builds the operating model that keeps sovereignty auditable and scalable in production.

Capgemini's role also extends beyond modernization into monetization. As operators explore how to package sovereign cloud, sovereign AI and trusted local operations as external services, the challenge becomes as much commercial and operational as technical. Capgemini helps define the service catalog, target market, operating model and partner structure needed to turn sovereign capability into a viable line of business.

Why Capgemini specifically. The joint venture behind Bleu demonstrates production-scale experience of operating sovereign cloud with Microsoft in a regulated national context. Combined with deep telco transformation capability across OSS/BSS, network and cloud-native delivery, this gives Capgemini a credibility few advisory-led sovereignty propositions can match.

Microsoft provides the platform continuum; Capgemini assembles, integrates, operationalizes and, where required, runs the whole outcome.

11

Conclusion

Digital sovereignty is driven by geopolitical, technological and regulatory forces — but its real value lies in enabling telcos to scale AI, protect their assets and unlock new growth. The operators that may be better positioned to compete are not those that pursue maximum isolation everywhere, nor those that treat sovereignty as a contractual afterthought. They will be the operators that engineer sovereignty selectively and visibly across the estate, using it to unlock innovation precisely where trust is hardest to establish.

As a consumer of sovereignty (to modernize), an operator should adopt hyperscale cloud as the primary platform for most workloads, engineer sovereignty selectively by sensitivity, and apply full sovereign control only where lawful intercept, critical national infrastructure or national-security mandates demand it. As a provider of sovereignty (to monetize), those same capabilities allow the operator to reposition as a trusted supplier of sovereign cloud, sovereign AI and national digital capacity.

Microsoft provides the platform continuum to implement this — from assured hyperscale through by-design, national partner clouds and sovereign-private environments; all anchored in a consistent control plane and sovereign AI capability. Capgemini enables clients to orchestrate the right balance across all domains of the digital value chain, manage reversibility and exit, integrate the wider ecosystem, and turn sovereignty into a working transformation and growth agenda.

Risks of getting it wrong

Over-control	Under-control
Cost inflation — a sovereign premium applied to workloads that never required full isolation.	Legal exposure — external jurisdictional reach into sensitive data and operations.
Innovation stagnation — AI, autonomous operations and 5G monetisation constrained by excessive controls.	Regulatory non-compliance — inability to demonstrate sovereign control of lawful intercept and critical workloads.
Operational complexity — multiple sovereign-only platforms create duplicated controls and permanent integration cost.	License risk — in certain cases, failure to demonstrate compliance may create regulatory risk affecting operations.
Competitive asymmetry — over-controlled operators cannot afford to scale the very sovereign services they aim to sell.	Competitive asymmetry — under-controlled operators cannot credibly compete for government, defense-adjacent or regulated-enterprise opportunities.

Sovereignty as a competitive advantage

The operators who win the next planning cycle will be those who stop debating whether to be sovereign and start engineering where to be sovereign. When effectively implemented, sovereignty can act as a commercial differentiator, not just a compliance cost.

Microsoft brings a strong sovereign-capable platform and control architecture. Capgemini brings the impartial orchestration, telco transformation depth, sovereign operating experience through Bleu, and ecosystem reach to turn that platform into an end-to-end result while keeping the client’s options open as the market evolves. Microsoft is how it is built; Capgemini is how it is made to work.



12

Proposed Next Step: The Telco Sovereignty Maturity Assessment

For telco operators, the next step is not the production of a maturity score in isolation. It is the ability to truly consider the sovereignty spectrum; and the value, regulatory confidence and future growth opportunities it can enable.

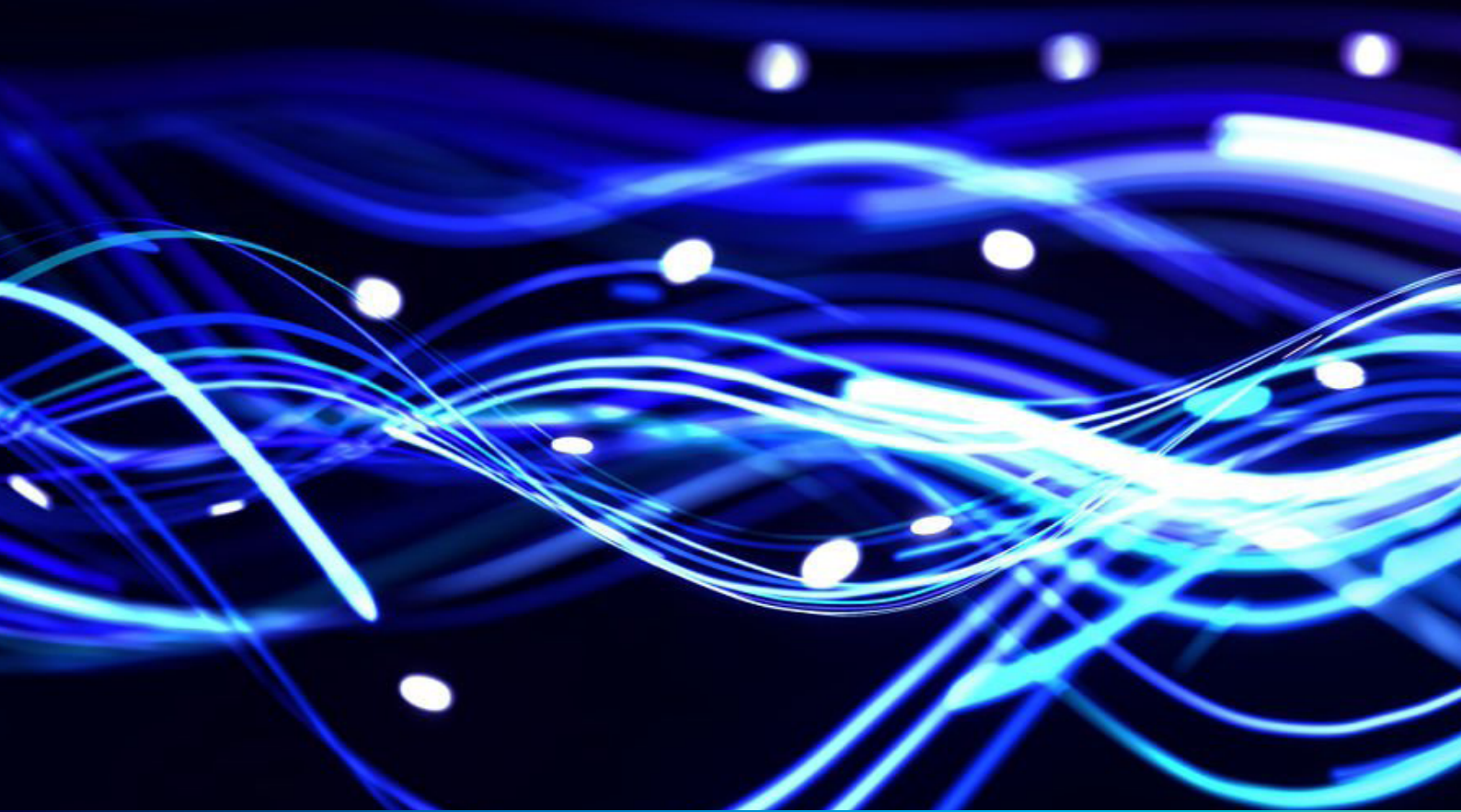
That is why the joint Capgemini–Microsoft assessment remains the right entry point. It gives leadership a

practical basis to determine which workloads belong in a by-design cloud model, which require stronger sovereign control, and where sovereign capability can support both modernization and, where relevant, monetization.

Approach for Telco	Activity	Deliverable	Value
1) Know where you stand	Explore where things are - current cloud estate, workload landscape, regulatory obligations, AI ambitions and sovereignty requirements; baseline against spectrum / SEAL model.	Current-state assessment and maturity baseline.	• Exposes control gaps across customer, OSS/BSS, AI and critical operational domains. • Gives leadership a single view of regulatory, resilience and license-to-operate pressure. • Creates a credible starting point for cloud and AI decisions.
2) Focus where it matters	Dig into the detail – workload suitability, risk exposure and control requirements.	Workload assessment and prioritized recommendations.	• Distinguishes workloads suited to assured hyperscale from those needing stronger sovereign control. • Reduces the risk of over-controlling low-risk workloads or under-controlling sensitive ones. • Turns sovereignty into a placement decision that supports speed, compliance and economics.
3) Build the model with confidence	Shape the approach - target-state operating model, governance, deployment patterns and reversibility / exit requirements.	Target-state architecture and sovereignty operating model.	• Defines how identity, policy, audit, resilience and exit work across the estate. • Avoids fragmented control models and parallel compliance functions. • Creates a scalable route across hybrid, sovereign-private and multi-market environments.
4) Set out the path	Create a clear direction - phased implementation roadmap, investment view, partner model and priority initiatives.	Executive-ready roadmap and business case.	• Sequences where to modernize first, where to harden first and where to defer. • Links sovereignty choices to AI enablement, service assurance and investment timing. • Gives ExCo a business case for action, not another strategy paper.
5) Make this real.	Turn plan in to reality - trusted partnership, assisted delivery, implementation, integration and adoption.	A sustainable and modern sovereign capability.	• Converts the approved model into a working capability through trusted partnership and assisted delivery. • Accelerates adoption across platform, integration and operating model change. • Builds a sustainable, modern capability rather than a one-off program artefact.

The outcome is therefore not a generic maturity score. It is a telco decision framework — and, with implementation support, a practical route to execution:

where to apply sovereignty selectively, how to modernize with greater confidence, and how to convert trusted control into enterprise value.



Bleu (Capgemini, Orange and Microsoft) – Sovereign Cloud for France

Strategic rationale - Bleu was established to address France's growing requirement for cloud services that combine hyperscale innovation with strict national sovereignty. The venture responds to board-level concerns around data exposure to foreign jurisdictions, control of critical digital infrastructure, and the need for high cyber resilience in sensitive sectors. It is designed to remove the traditional trade-off between cloud innovation and sovereign control.

What the solution provides - Bleu is a sovereign trusted cloud platform, created as a joint venture between Capgemini and Orange in strategic partnership with Microsoft. It delivers Microsoft Azure and Microsoft 365 through a French-controlled cloud environment, enabling organizations to access leading cloud and productivity capabilities while operating within a framework aligned to French and European sovereignty requirements.

Sovereignty model and critical components - Bleu's value proposition is underpinned by a multi-layered sovereignty model spanning:

- Legal sovereignty – data and services governed under French and EU jurisdiction
- Operational sovereignty – independent operations under European control

- Technical sovereignty – a re-engineered cloud environment designed specifically for sovereign use
- Cybersecurity and compliance – built to a compliance-first model, targeting ANSSI SecNumCloud (in 2027), France's highest cloud security standard

This architecture enables Microsoft cloud services to be delivered in a way that aligns with the needs of organizations where sovereignty is a non-negotiable requirement.

Target sectors and use cases - Bleu is aimed at organizations operating in highly sensitive and regulated environments, including:

- French State institutions and public agencies
- Hospitals and regional authorities
- Vital Importance Operators (OIVs)
- Essential Service Operators (OSEs)
- Other regulated or critical infrastructure sectors

The primary use case is enabling these organizations to adopt Microsoft 365 and Azure at scale without compromising on sovereignty, data residency, or regulatory compliance.

Bleu represents a strategically important model for the European cloud market: a sovereign hyperscale platform that combines the innovation, scale and productivity benefits of Microsoft cloud services with national legal, operational and infrastructure control. It demonstrates how telecom and technology partnerships can create trusted digital foundations for critical sectors.



2. Telenor and Capgemini – Sovereign AI for Norway and the Nordics

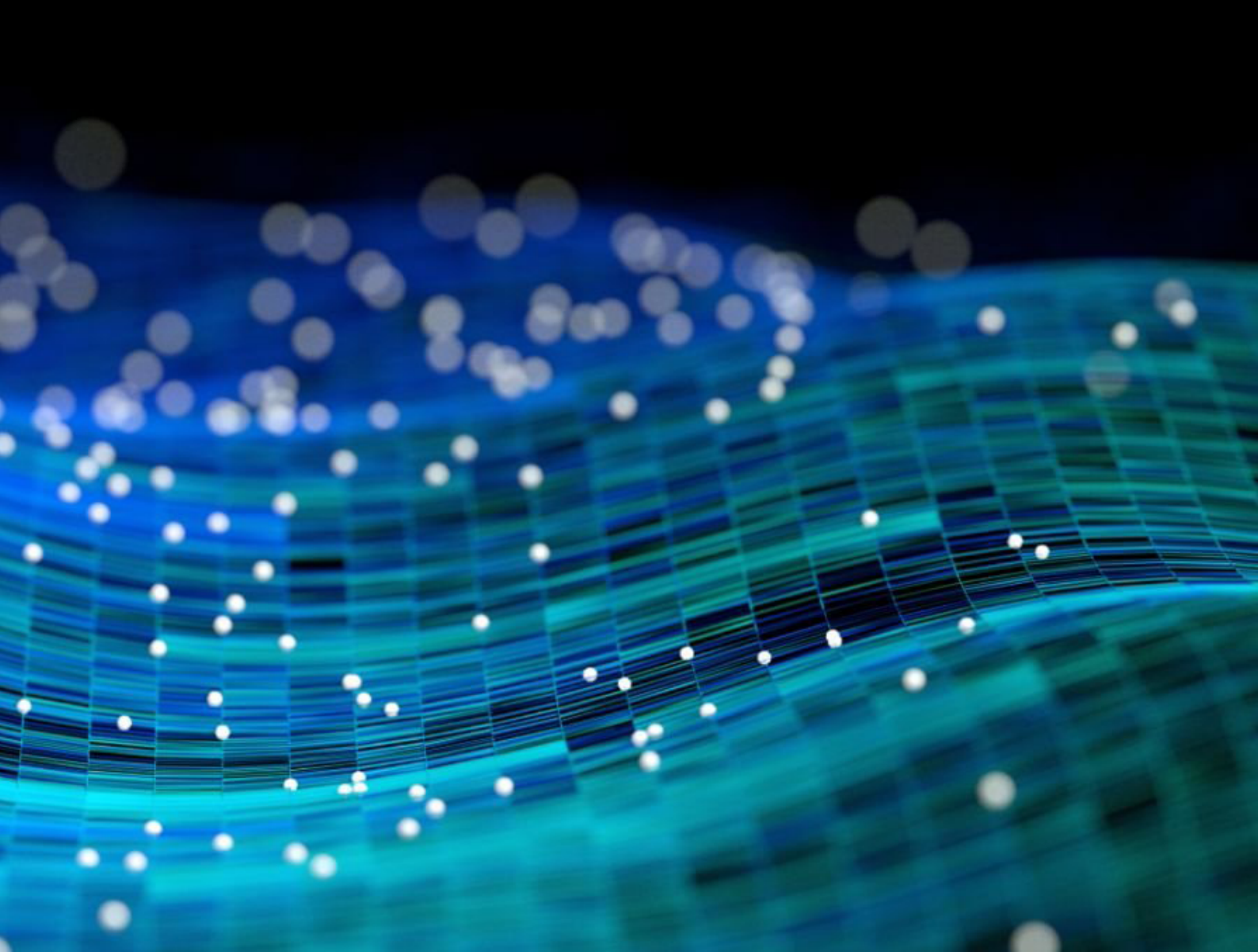
Strategic rationale – The combination of Telenor and Capgemini reflects a response to the growing demand for sovereign AI in Europe. It supports Telenor's evolution from a traditional connectivity provider to a broader technology-led digital services player. This capability is designed to help enterprises and public-sector organisations harness AI-services while maintaining local control of sensitive data, ensuring compliance, resilience and trust.

What the solution provides - At the centre of the collaboration is Telenor AI Factory, Norway's first sovereign AI cloud platform. Building upon a Telenor business need for Sovereign AI, the platform evolved to host AI workloads securely, ensure data remains within national borders, and provide a foundation for enterprise and public-sector AI adoption. Capgemini brings AI and data expertise and transformation

capabilities. Telenor contributes infrastructure, telecom domain expertise and market access, in line with a joint GTM approach.

Sovereignty model and critical components – is a combination of infrastructure and services to deliver a sovereign AI proposition built on:

- Data sovereignty – AI workloads and sensitive data processed within Norway
- Secure and sustainable infrastructure – a trusted platform for enterprise and public-sector AI
- End-to-end co-creation – from business case design and platform build through to operations and scaling
- Governance and compliance – frameworks to support responsible, regulated and scalable AI adoption
- Telecom-enabled AI innovation – applying AI to network automation, optimisation and service transformation



This is more than a technology deployment; it is a strategic operating model for sovereign AI enablement.

Target sectors and use cases - The offering is targeted at Norwegian and wider Nordic enterprises, governments and public-sector organisations, particularly those with regulated, sensitive or strategically important data. Key use cases include:

- BabelSpeak (Capgemini solution) – real-time translation across 100+ languages, including humanitarian applications such as Red Cross support
- AI-driven telecom innovation (Telenor) – including network automation and optimisation and general efficiency of AI on sensitive, regulated data
- Enterprise AI services (joint GTM agreement) – AI strategy, advisory, deployment frameworks, and governance models

This is not a conventional outsourcing arrangement or fixed-scope IT contract. It is a strategic co-innovation launch, operations and joint go-to-market model, bringing together platform capability and transformation services to create a sovereign AI ecosystem. It illustrates how telcos can move up the value chain by monetising secure digital infrastructure, trusted data environments and AI-enabled services.

Contacts



Capgemini

Praveen Shankar

Global Head of Telecommunications,
Capgemini
praveen.shankar@capgemini.com



Thilo Ewald

CTO Telco Germany, Capgemini
thilo.ewald@capgemini.com



Mark Kennedy

Senior Cloud & Platform Lead,
Capgemini
mark.kennedy@capgemini.com



Microsoft

Alessandra Antonelli

Global Strategy and Solutions,
Telecommunications Industry,
Microsoft
alantonelli@microsoft.com



Rick Lievano

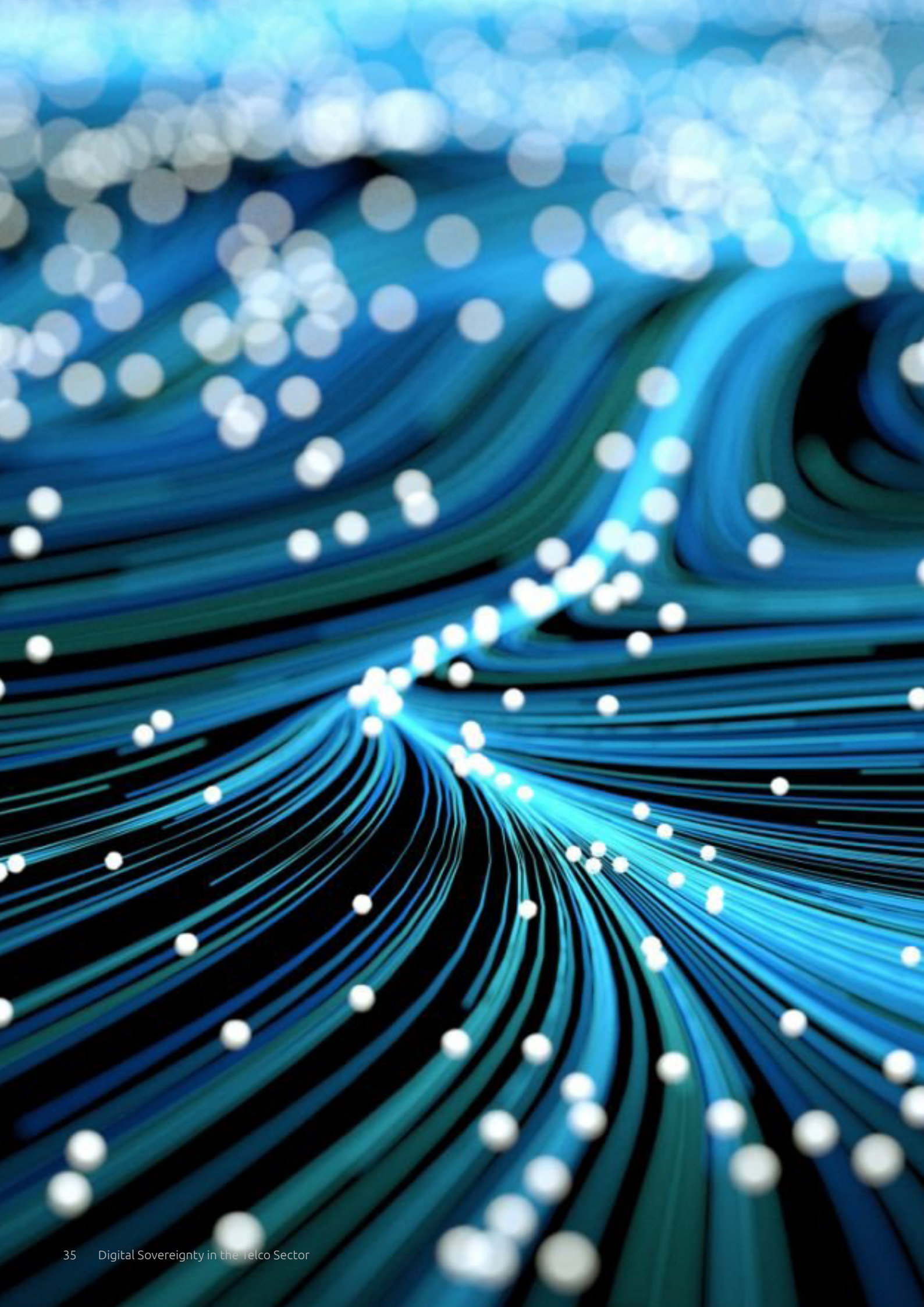
CTO, WW Telecommunications
Industry, Microsoft
rickliev@microsoft.com



Richard Cheney

Senior Partner Solutions Architect,
Microsoft
richard.cheney@microsoft.com





About Capgemini

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of over 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2025 global revenues of €22.5 billion.

Make it real | www.capgemini.com

