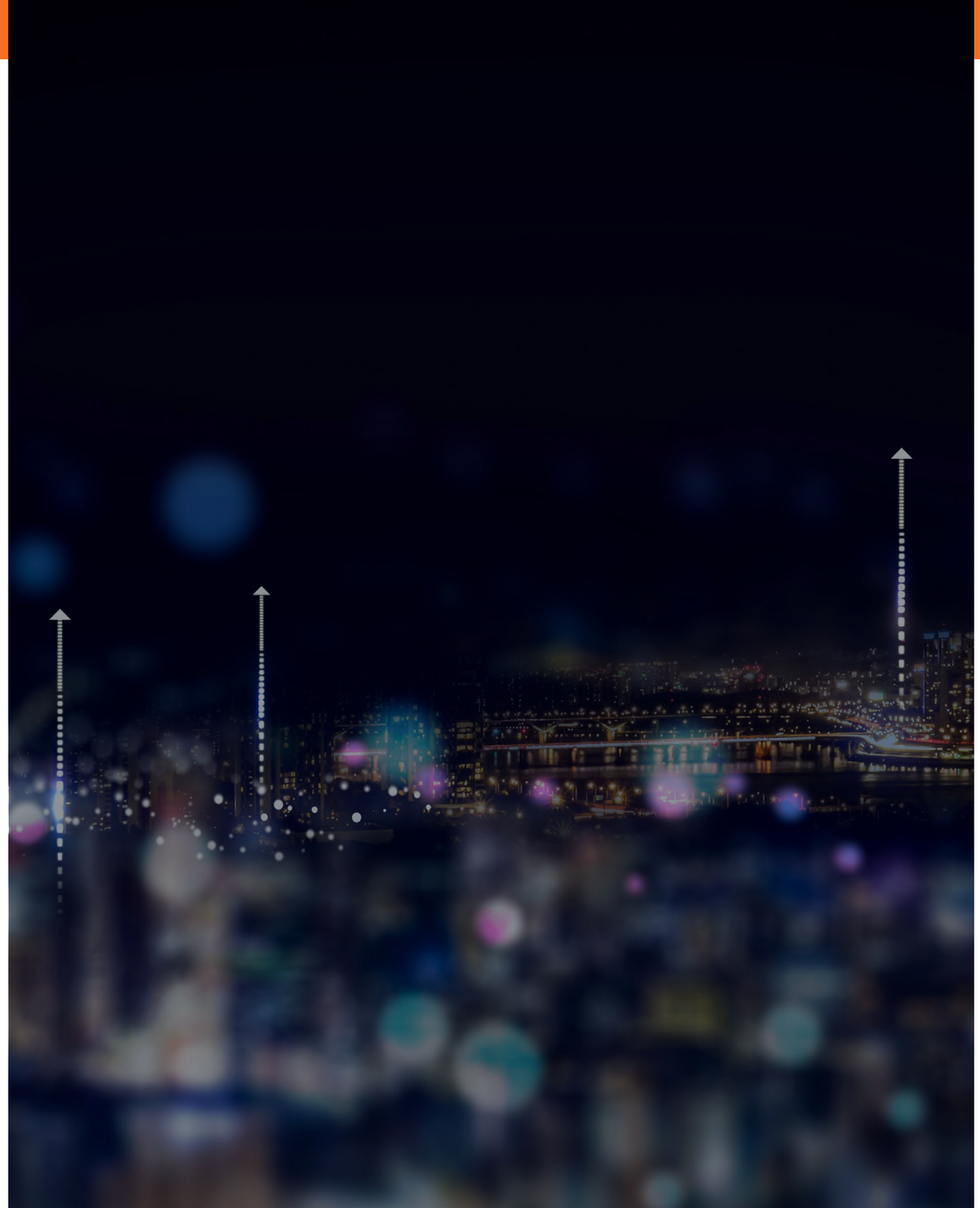
CLOUDERA

www.cloudera.com

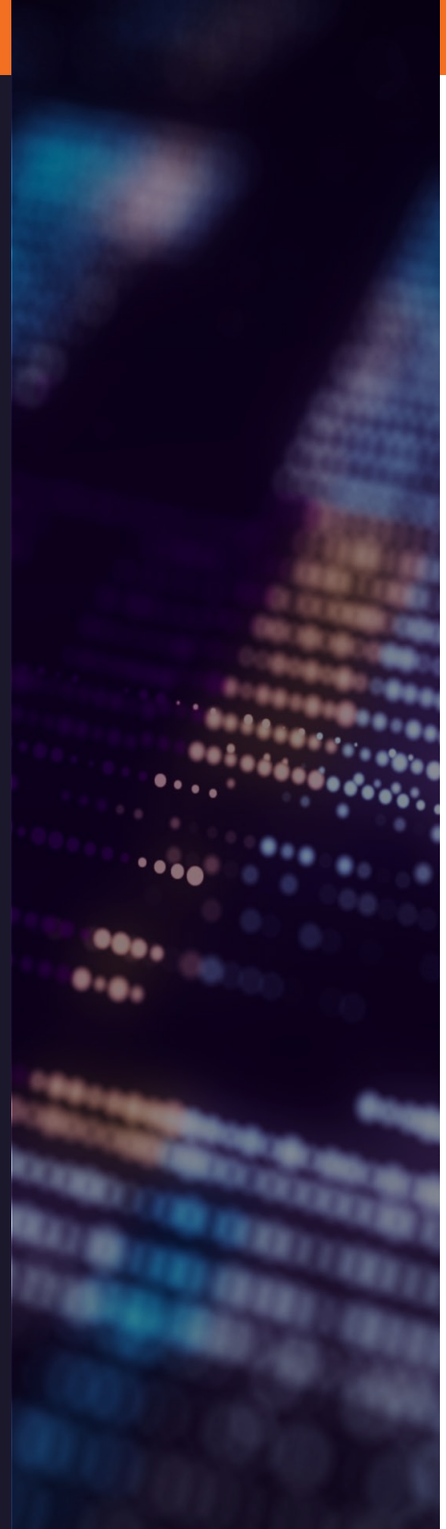


SOVEREIGNTY AS STRATEGY

BUILDING TRUST, CONTROL, AND INNOVATION IN THE AI ERA

A guide to digital sovereignty in practice

TABLE OF **CONTENTS**



CLOUDERA

EXECUTIVE **SUMMARY**

The global sovereign cloud market is projected to surge from $154.69 billion in 2025 to $823.91 billion by 2032 – a 27 per cent compound annual growth rate that signals a fundamental shift in how organisations approach data infrastructure. This growth reflects an urgent imperative: in an era of tightening regulations, geopolitical uncertainty, and AI transformation, sovereignty has evolved from a compliance checkbox to a strategic enabler of trust, innovation, and competitive advantage.

Sovereignty operates across three interconnected pillars: digital infrastructure, data control, and AI deployment. Success requires modern, open platforms that deliver control without constraint: architectures built on openness to prevent lock-in, hybrid flexibility for operational choice, comprehensive governance for compliance, and support for sovereign AI innovation. The organisations making the right architectural decisions today will determine their freedom of action tomorrow.

Section 1

THE SOVEREIGNTY IMPERATIVE
WHY SOVEREIGNTY MATTERS NOW, AND WHAT'S CHANGED

Digital sovereignty has moved from the periphery to the centre of boardroom and government decision-making. What began as a data protection concern has expanded into a broader question of strategic autonomy: the ability of nations and organisations to operate, innovate, and compete without undue dependence on external powers. This encompasses not only control over data and infrastructure, but resilience against geopolitical disruption, legal exposure to foreign jurisdictions, and external shocks across critical supply chains, from energy to trade.

For organisations, this shift is reshaping how technology infrastructure is built, deployed, and governed. The sovereign cloud market's projected growth to $823.91 billion by 2032 reflects more than rising compliance requirements and signals a structural recalibration of priorities across industries and nations, as digital infrastructure becomes inseparable from economic security and long-term competitiveness.[^1]

Three converging pressures are driving this transformation.

Regulatory and geopolitical forces have elevated sovereignty from compliance concern to operational necessity. Beyond GDPR's data protection framework, the EU Data Act mandates portability and interoperability, whilst sector-specific regulations like MiFID II and PCI DSS narrow margins for error. GDPR fines can reach 4 per cent of global turnover. Simultaneously, nations and regional blocs actively reduce dependence on foreign technology infrastructure, driven by concerns about surveillance and economic leverage. In 2024, 72 per cent of European businesses prioritised data sovereignty when selecting technology vendors.[^2]

Customer trust has emerged as a tangible competitive differentiator, but its foundations extend beyond conventional data protection. From a consumer perspective, frameworks such as GDPR are designed to safeguard privacy, but on a higher level they also limit exposure to foreign legal regimes and reduce the risk of external influence over sensitive data and digital services. Sovereignty therefore un-

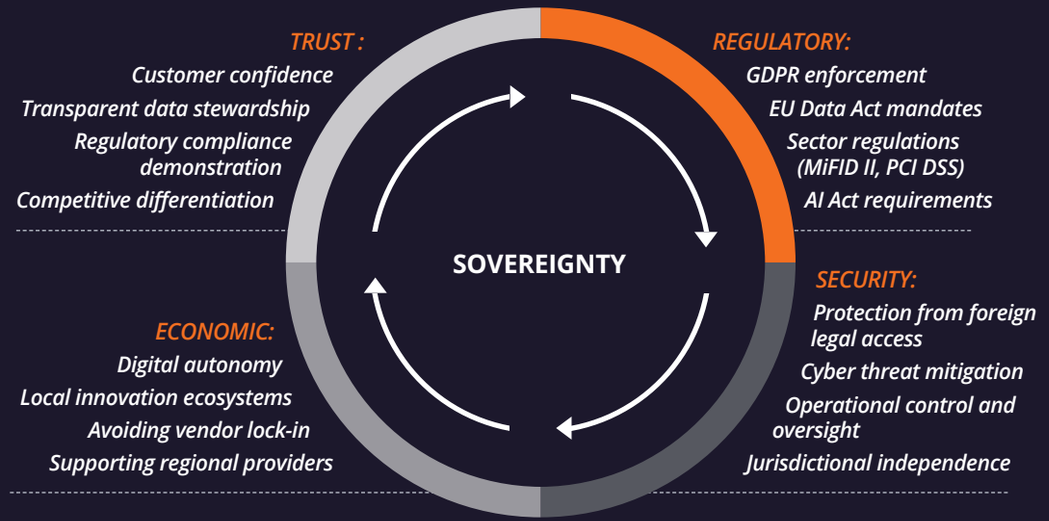
derpins confidence that data is governed within accountable, domestic frameworks. Organisations that keep data within recognised legal and geographical boundaries and are under appropriate jurisdictional control signal resilience against external access. In heavily regulated sectors like financial services and healthcare, this assurance translates directly into client retention, regulatory approval and sustained market access.

AI governance has introduced new sovereignty imperatives. As organisations deploy generative AI and large language models, questions of who controls training data, where models execute, and how insights are governed have become critical. Years of underinvestment have left regions such as Europe heavily dependent on non-domestic hyperscalers for AI infrastructure, concentrating capability outside local jurisdictional control. The EU's "AI Continent Action Plan", including ambitions to triple data centre capacity, reflects growing recognition that AI is a strategic asset.

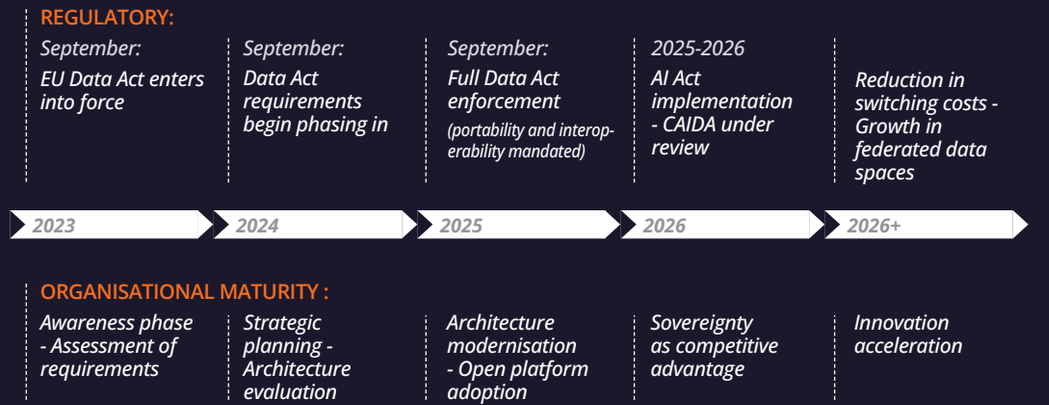
Without sovereign control, organisations risk data exposure and increasing reliance on external providers for core decision-making, automation, and digital capabilities.

The shift in organisational mindset is uneven. In practice, many executives continue to prioritise near-term outcomes, cost reduction, performance, and time-to-value over longer-term considerations such as portability or jurisdictional flexibility. This is evident in continued concentration on hyperscaler platforms and tightly integrated services, even in regulated sectors. However, this tactical focus can create structural dependencies that are difficult to unwind as regulatory and geopolitical pressures intensify. Non-compliance risks substantial fines, operational disruptions, and market exclusion. Organisations that align short-term optimisation with sovereignty-ready architectures are better positioned to retain flexibility, enable market access, and build trust as a source of competitive advantage.

THE SOVEREIGNTY DRIVERS



THE DATA ACT IMPACT TIMELINE



Section 2

THE THREE PILLARS OF SOVEREIGNTY – **UNDERSTANDING THE SOVEREIGNTY CONTINUUM**

> ***Sovereign cloud offerings increasingly feature dedicated infrastructure, local operational teams, and contractual protections designed to create legal and technical barriers against foreign access.***

SOVEREIGN CLOUD
THE FOUNDATION

2.1

Cloud sovereignty encompasses the infrastructure and operational frameworks that ensure data residency, local operational control, and protection from foreign legal frameworks. It represents the foundational layer upon which data and AI sovereignty are built.

The core requirements are clear. Geographic location matters: physical data centres must reside within defined national or regional borders. Local operational teams and governance structures ensure that personnel managing infrastructure are subject to domestic laws and oversight. Legal jurisdiction alignment guarantees that cloud providers and their operations fall under regional regulatory frameworks, not foreign statutes like the US CLOUD Act. Operational independence means that sensitive systems remain insulated from external government access or economic leverage.

The challenge lies in balancing sovereignty with global operational needs and cloud economics. Organisations require the scale, efficiency, and innovation velocity of cloud computing whilst maintaining jurisdictional control over critical data and systems. This tension has driven the emergence of sovereign cloud offerings from major providers, including AWS European Sovereign Cloud, alongside national and regional alternatives.

A critical question persists: can US hyperscalers deliver true sovereignty despite home country laws? The answer lies in operational separation and legal safeguards. Sovereign cloud offerings increasingly feature dedicated infrastructure, local operational teams, and contractual protections designed to create legal and technical barriers against foreign access. Yet some regulators and organisations maintain that authentic sovereignty requires fully EU-owned or nationally controlled providers.

DATA SOVEREIGNTY
THE CONTROL LAYER

2.2

Data sovereignty extends beyond infrastructure to encompass comprehensive oversight and governance of citizen and customer data privacy across their entire lifecycle. Whilst digital sovereignty addresses where systems operate, data sovereignty governs what happens to information itself: how personal and sensitive data is accessed, processed, and protected within jurisdictional boundaries. This includes ownership, processing rights, cross-border movement controls, and, critically, portability. In this context, privacy is not an isolated concern but a core expression of sovereignty, ensuring that data remains subject to trusted legal frameworks and insulated from unauthorised external access or influence.

The EU Data Act's mandate for interoperability and elimination of switching fees has elevated portability from technical concern to legal requirement. Organisations must be able to move data between environments without prohibitive costs or proprietary lock-in. This portability imperative carries profound architectural implications.

Modern approaches centre on the data lakehouse architecture supporting standardised, interoperable table formats that enable controlled sharing without moving data. This distinction is critical: rather than copying or transferring data across boundaries, data remains exactly where it is, physically located within jurisdictional boundaries, whilst multiple processing engines securely access it through standardised interfaces. This "compute-to-data" model allows analytics and AI workloads to operate on sovereign data without requiring physical transfer or duplication, fundamentally changing the sovereignty equation.

Unified governance across on-premises and cloud environments ensures consistent security policies, access controls, and audit trails regardless of where workloads execute. Customer-controlled encryption and key management through bring-your-own-key (BYOK) or hold-your-own-key (HYOK) models ensure that even infrastructure providers cannot access sensitive data without explicit authorisation.

The federation vision extends these principles across organisational boundaries. Data mesh principles, people and process supported by technology to create and share data as products, enable faster innovation whilst maintaining sovereignty. Secure data spaces allow controlled sharing without physical transfer, supporting collaboration in strategic industries whilst respecting ownership and jurisdictional requirements.

The alternative – proprietary formats and closed APIs – create sovereignty barriers. Vendor lock-in through incompatible data structures forces organisations to choose between maintaining current infrastructure (with escalating costs and diminishing innovation) or undertaking expensive, risky migrations. In a sovereignty context, this technical lock-in becomes a strategic vulnerability.

THE SOVEREIGNTY CONTINUUM IN PRACTICE

SCENARIO:
European financial services provider

Cloud sovereignty:
Partners with European sovereign cloud provider with data centres in Frankfurt, German operational teams, and EU legal jurisdiction.

Data sovereignty:
Implements open lakehouse architecture with Apache Iceberg for portability; customer-controlled encryption; all transaction data within EU whilst enabling cross-border analytics where permitted.

Sovereign AI:
Trains fraud detection models on local data; maintains full control over model updates; leverages open-weight LLMs for auditability and responsible AI.

Outcome:
Regulatory compliance + customer trust + innovation capability

> *Sovereign AI enables localised innovation, sector-specific models tailored to regional needs, and competitive differentiation based on trustworthy, auditable AI systems*

SOVEREIGN AI
THE INNOVATION FRONTIER

2.3

Sovereign AI represents the most transformative dimension of the sovereignty continuum. It encompasses AI development and deployment – including data, models, prompts, and outputs – within controlled, trusted perimeters. As AI becomes central to economic competitiveness and national security, sovereignty over these systems has emerged as a strategic imperative. This extends beyond infrastructure to ownership and control of the intelligent agents and automation capabilities reshaping digital work. It also underpins the ability to drive frontier innovation and ensure AI systems reflect local languages, cultural context, and regulatory values, rather than those defined externally.

The stakes are increasingly defined by economic and societal outcomes. AI will reshape regional government policies on education, skills development, employment structures, and social services. It stands poised to accelerate breakthroughs in frontier sciences: fusion energy, carbon capture, quantum computing. In this landscape, each region and nation competes to reach transformative capabilities first. AI constitutes a strategic national and organisational asset in the most literal sense.

Dependency on foreign AI infrastructure creates risks across multiple dimensions: models trained on data outside jurisdictional control, updates deployed without oversight, and insights flowing to external parties. Nations investing in sovereign AI infrastructure recognise that losing control over AI capabilities means ceding advantage not merely in sectors like healthcare, defence, and financial services, but potentially in determining the trajectory of societal development itself.

Key capabilities define sovereign AI readiness. Local model training and fine-tuning on sovereign data ensures AI systems reflect domestic contexts and regulatory requirements. Control over model updates and lifecycle prevents autonomous third-party changes that could alter behaviour or compromise compliance, critical as AI systems automate sensitive decisions in credit evaluation, medical diagnosis, and public services. Federated learning enables collaborative innovation, allowing organisations to collectively train models whilst keeping data within sovereign boundaries, supporting breakthrough research whilst preserving privacy. Auditability and explainability grow more pressing as frameworks like the EU AI Act impose transparency requirements. Real-world examples illustrate this approach: Humain, for instance, hosts AI models within Saudi Arabia, enabling enterprises, public institutions, and developers to comply with national data sovereignty regulations without transferring sensitive data abroad. [^3]

The EU's "AI Continent Action Plan" and investments in sovereign AI infrastructure reflect recognition that AI represents a transformative frontier. The plan aims to triple data centre capacity, supporting development of AI capabilities within European jurisdictional and ethical frameworks. This isn't merely about compliance. Sovereign AI enables localised innovation, sector-specific models tailored to regional needs, and competitive differentiation based on trustworthy, auditable AI systems.

Beyond regulatory compliance, sovereign AI unlocks possibilities: financial institutions developing fraud detection models on local transaction patterns, healthcare systems training diagnostic AI on regional patient populations, governments deploying citizen services powered by culturally appropriate language models. Each represents innovation impossible without sovereign control over data, infrastructure, and AI capabilities.

MYTHS VS. REALITY

SOVEREIGNTY MISCONCEPTIONS

	Myths	*Reality*
1	Sovereignty means avoiding public cloud entirely	Sovereign cloud offerings from major providers, combined with open platform architectures, enable sovereignty with cloud benefits
2	Sovereignty is only about data location	It encompasses operational control, legal jurisdiction, encryption management, and portability, not just geography
3	Sovereignty kills innovation	Sovereign AI frameworks support localised innovation, federated learning, and competitive differentiation, while ensuring AI reflects regional culture, values, and regulatory requirements – illustrated by examples such as Humain, which hosts models locally to comply with Saudi Arabia's data sovereignty rules.
4	Sovereignty is too expensive for most organisations	While smaller sovereign providers may face challenges achieving scale – leading to potential consolidation or market aggregation – sovereignty can still deliver positive ROI when factoring in avoided compliance costs, gained market access, and the elimination of switching penalties. Organisations can benefit economically while remaining mindful of provider stability and long-term market dynamics.
5	Open-source compromises security in sovereign environments	Proprietary foundations are not the only option for secure, auditable, and interoperable sovereign environments. Open, standards-based architectures can reduce hidden dependencies and vendor lock-in, supporting collaboration while maintaining control.

Section 3

ARCHITECTURAL REQUIREMENTS FOR SOVEREIGNTY: WHAT ORGANISATIONS NEED FROM THEIR DATA PLATFORMS

Traditional proprietary platforms fundamentally undermine sovereignty objectives. Switching costs function as sovereignty barriers, trapping organisations in infrastructure relationships that may become untenable as regulations evolve or geopolitical circumstances shift.

Limited portability compromises data control: if data cannot move freely between environments without format conversion or application re-architecture, organisations face a choice between accepting vendor terms or undertaking disruptive, costly transitions. Opaque operations that obscure how data is processed or who holds encryption keys create accountability gaps incompatible with sovereignty principles. As specialised regional providers emerge, platforms providing genuine portability become essential to preventing sovereignty solutions from creating new dependencies.

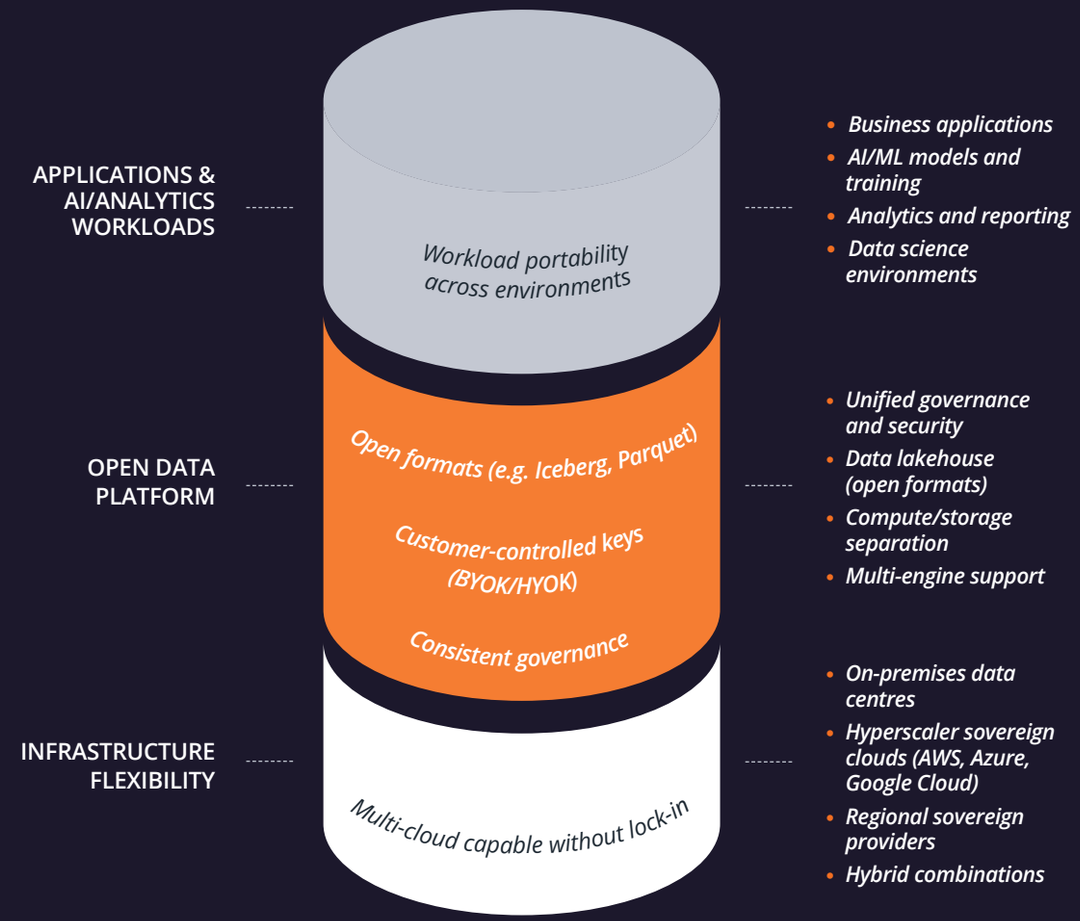
Four essential capabilities define sovereignty-ready platforms.

First, platforms must prioritise openness and interoperability through standards and architectural design rather than specific technologies. Support for flexible data formats and abstractions ensures that data remains accessible across processing engines and environments without proprietary lock-in. Organisations can leverage data spaces and data cleanrooms to enable controlled collaboration, secure sharing, and governance across domains while maintaining sovereignty. Certification against recognised sovereignty standards provides assurance that platforms meet the technical, legal, and operational requirements essential in sovereign contexts.

Second, platforms must enable workload portability and consistent governance across the environments organisations actually operate in, whether cloud or on-premises during transitional phases. Applications and data should be managed to maintain sovereignty, security, and operational control without dependence on proprietary infrastructure. Support for isolated

SOVEREIGNTY-READY ARCHITECTURE BLUEPRINT

3.1



or air-gapped deployments ensures that highly regulated or sensitive workloads remain protected, while integration with multiple infrastructure providers preserves choice and prevents vendor lock-in as organisations rationalise their data estates and move to cloud-first models.

Third, separation of compute and storage, enabling independent scaling for sovereignty and efficiency. Organisations can maintain sovereign storage within jurisdictional boundaries whilst leveraging compute resources where regulations permit or operational requirements dictate. This separation proves essential for "compute-to-data" models in federated scenarios, where processing occurs on data without requiring physical transfer across boundaries.

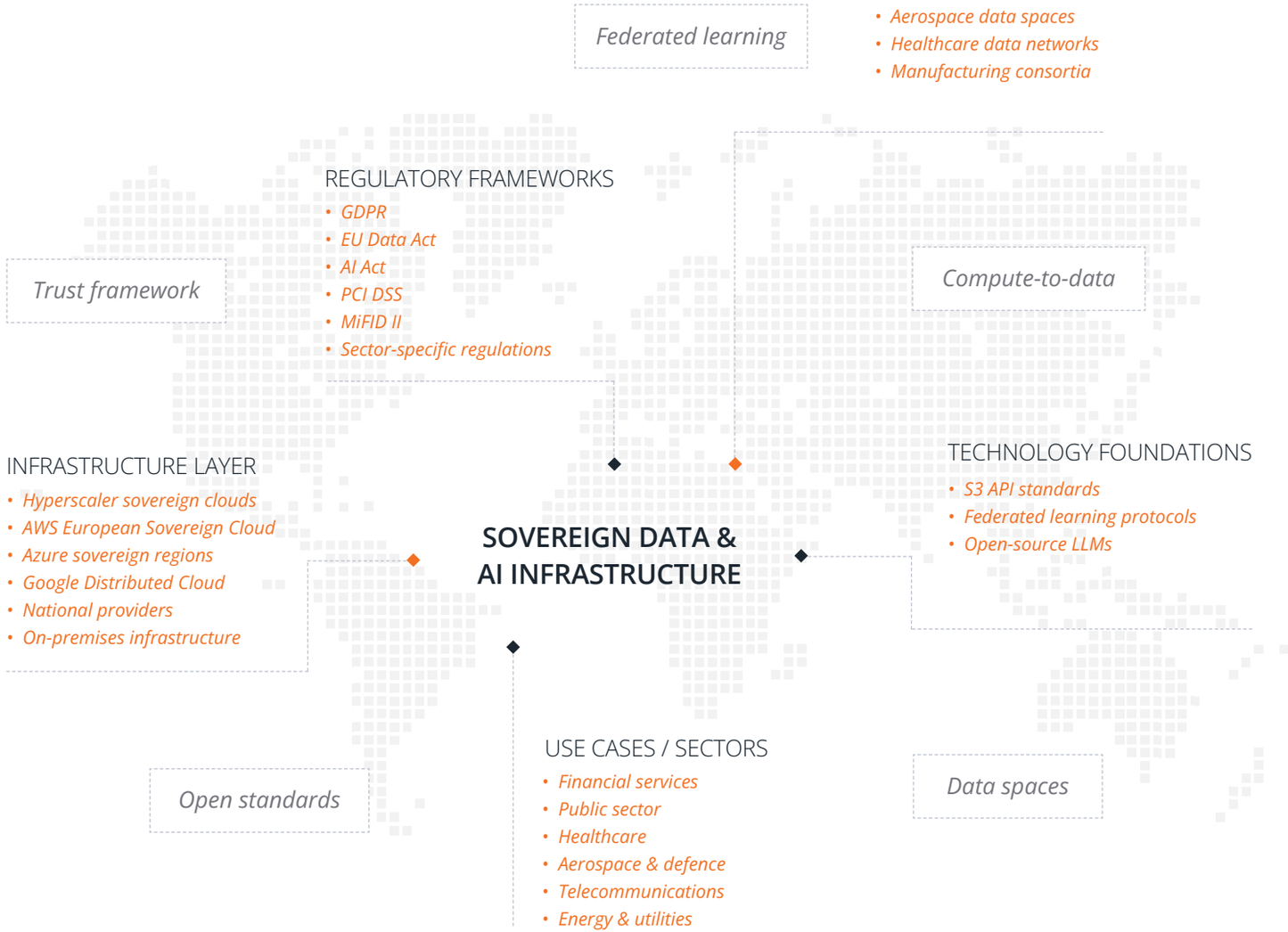
Fourth, comprehensive governance through unified security and access controls across environments, ensuring consistent policy enforcement regardless of where data or workloads reside. Customer-controlled encryption and key management through BYOK and HYOK models place cryptographic control firmly in organisational hands. Detailed audit trails enable compliance demonstration, whilst data lineage and classification capabilities support governance requirements across complex, multi-environment deployments.

Working with hyperscalers whilst maintaining sovereignty represents practical reality for most organisations. Leveraging AWS, Azure, and Google Cloud sovereign regions as infrastructure provides access to global scale, innovation, and operational expertise. The European Sovereign Cloud from AWS, representing a $7.8 billion investment in a $78 billion addressable market, demonstrates hyperscaler commitment to sovereignty requirements.[^4]

The key lies in adding platform capabilities that enhance portability and control. Rather than viewing hyperscaler infrastructure as lock-in, organisations should deploy platforms that enable movement between providers whilst maintaining consistent data governance, security controls, and application architectures. This means prioritising open standards, portable data formats, and abstraction layers that insulate applications from infrastructure dependencies.

SOVEREIGNTY ECOSYSTEM MAP

3.2



EVALUATING PLATFORM VENDORS FOR SOVEREIGNTY

ESSENTIAL QUESTIONS FOR PROCUREMENT

3.3

ON DIGITAL SOVEREIGNTY:

- Can the platform operate in our chosen sovereign infrastructure?
- Does it support on-premises, hybrid, and multiple cloud providers?
- What dependencies exist on foreign-controlled services?

ON DATA SOVEREIGNTY:

- Are open data formats (e.g. Iceberg, Parquet) supported natively?
- Can we migrate data between environments without proprietary conversion?
- Who controls encryption keys: vendor or customer?
- What's the process and cost for data egress?

ON SOVEREIGN AI:

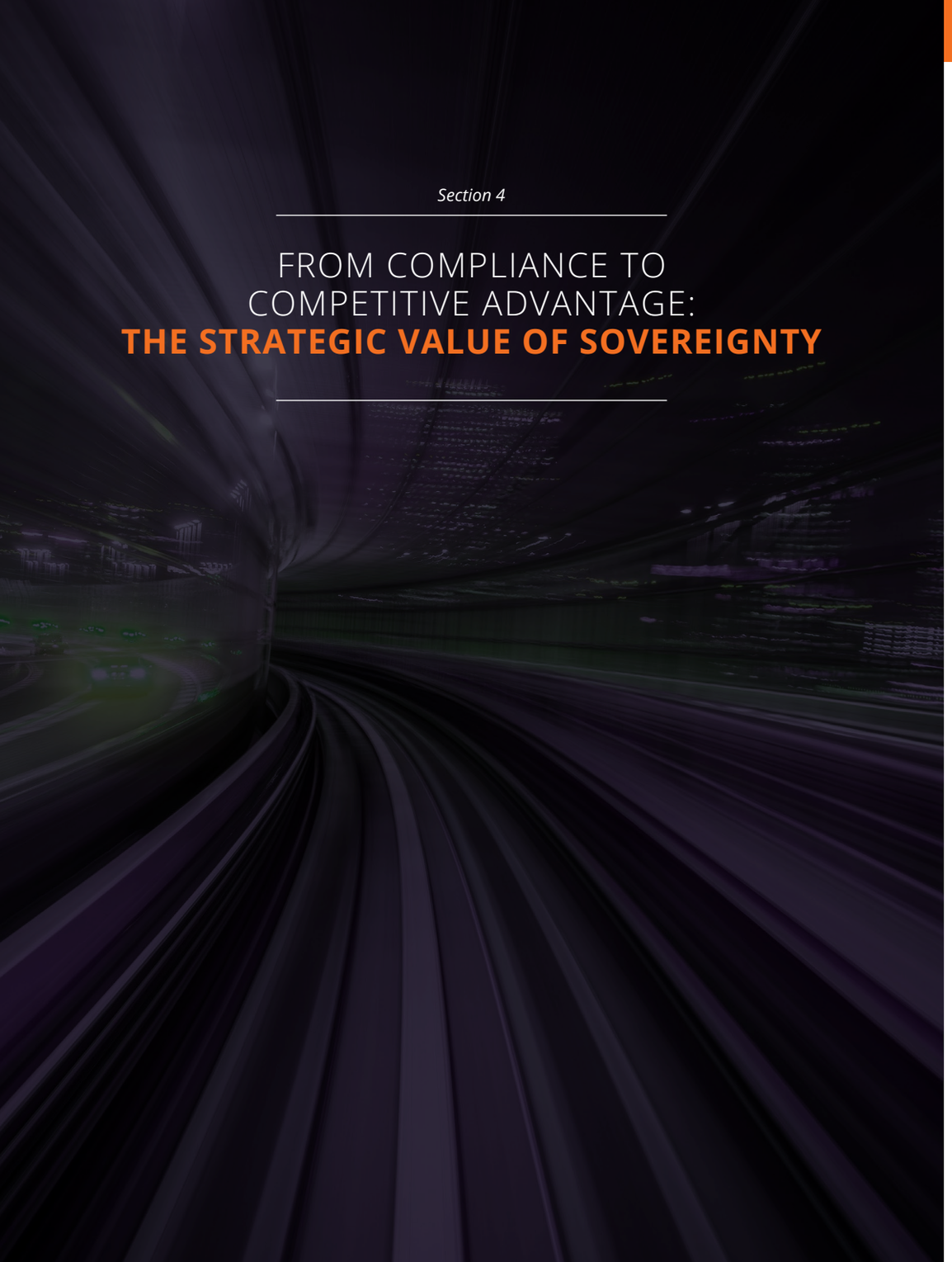
- Where do AI models execute: in our infrastructure or vendor's?
- Can we use open-source/ open-weight models we've audited?
- Who controls model updates and versioning?
- Is federated learning supported for multi-party scenarios?

ON GOVERNANCE & COMPLIANCE:

- Are audit trails comprehensive and exportable?
- Does the platform support data lineage and classification?
- What certifications exist for regulated industries?
- How does multi-tenancy isolation work?

ON STRATEGIC FIT:

- Does the vendor have a track record in sovereign deployments?
- Are they aligned with initiatives?
- What's their position on open standards vs. proprietary APIs?



Section 4

FROM COMPLIANCE TO COMPETITIVE ADVANTAGE: THE STRATEGIC VALUE OF SOVEREIGNTY

Sovereignty-ready architectures deliver value across four strategic dimensions, transforming what might appear as compliance burden into genuine competitive advantage.

$154.69B › $823.91B

Global sovereign cloud market growth projection (2025-2032) at 27% CAGR

Source: Fortune Business Insights (2024-2025)

MARKET ACCESS AND GROWTH

Sovereignty enables entry into regulated sectors and public contracts that require jurisdictional control. Organisations in regions with strict data localisation laws, from China to Russia and other assertive markets, rely on sovereign capabilities to maintain access and operations.

72% *European businesses prioritising data sovereignty in vendor selection (2024)*

Source: Hivenet (2025)

CUSTOMER TRUST AND DIFFERENTIATION

With 72 per cent of European businesses prioritising sovereignty in vendor selection, demonstrable data stewardship builds brand value and supports client acquisition and retention. In regulated sectors like financial services, healthcare, and legal services, sovereignty signals responsible custodianship of sensitive information.

INNOVATION VELOCITY

Sovereignty enables local AI development and sector-specific models, accelerating time-to-insight while avoiding compliance delays. Federated learning and controlled collaboration allow participation in industry research and benchmarking without compromising data ownership.

$70B *Predicted global government cloud spending by 2025 (tripling from previous levels)*

Source: Cloudera (2025), Navigating Data Sovereignty

3X *EU's AI Continent Action Plan aims to triple data centre capacity*

149 zettabytes

Global data generation by end of 2024

4% *Up to 4 per cent GDPR fines as percentage of global turnover for non-compliance*

ECONOMIC EFFICIENCY

Sovereign infrastructure reduces financial and reputational risk. GDPR fines reach up to 4 per cent of global turnover, while the EU AI Act adds penalties for prohibited practices or incorrect outputs, potentially compounding exposure. Compliance avoidance, secure operations, and elimination of switching costs deliver measurable savings. Investments in sovereign platforms also strengthen local digital economies, create skilled jobs, and support regional technology providers, generating broader social and economic value beyond individual organisational benefits.

Initial investments in sovereign infrastructure can exceed conventional cloud costs due to specialised facilities and compliance requirements. However, these investments deliver savings by avoiding GDPR and sector-specific fines, reducing breach remediation expenses, and unlocking market access and revenue streams that require jurisdictional compliance. Sovereign AI capabilities provide measurable innovation advantages. Technological trends such as distributed architectures and edge computing lower costs while maintaining compliance, and open, portable platforms enable organisations to adapt to evolving regulations without costly re-architecture, providing resilience against regulatory and geopolitical shifts.

THE SOVEREIGNTY MATURITY MODEL

WHERE DOES YOUR ORGANISATION STAND?

4.1

LEADERSHIP

Pioneering sovereign AI and federated ecosystem participation

- *Active participation in industry initiatives*
- *Sovereign AI in production*
- *Industry thought leadership*

STRATEGIC

Leveraging sovereignty for competitive advantage and innovation

- *Sovereignty as market differentiator*
- *Sovereign AI pilots underway*
- *Cross-border federated data sharing*

PROACTIVE

Implementing comprehensive controls (cloud + data sovereignty)

- *Open architecture deployed*
- *Customer-controlled encryption*
- *Multi-cloud portability established*

REACTIVE

Meeting minimum compliance (data location only)

- *Data residency achieved*
- *Basic regulatory compliance*
- *Limited strategic integration*

AWARE

Understanding regulatory requirements and basic risks

- *Regulatory assessment completed*
- *Risk identification underway*
- *Planning initiated*

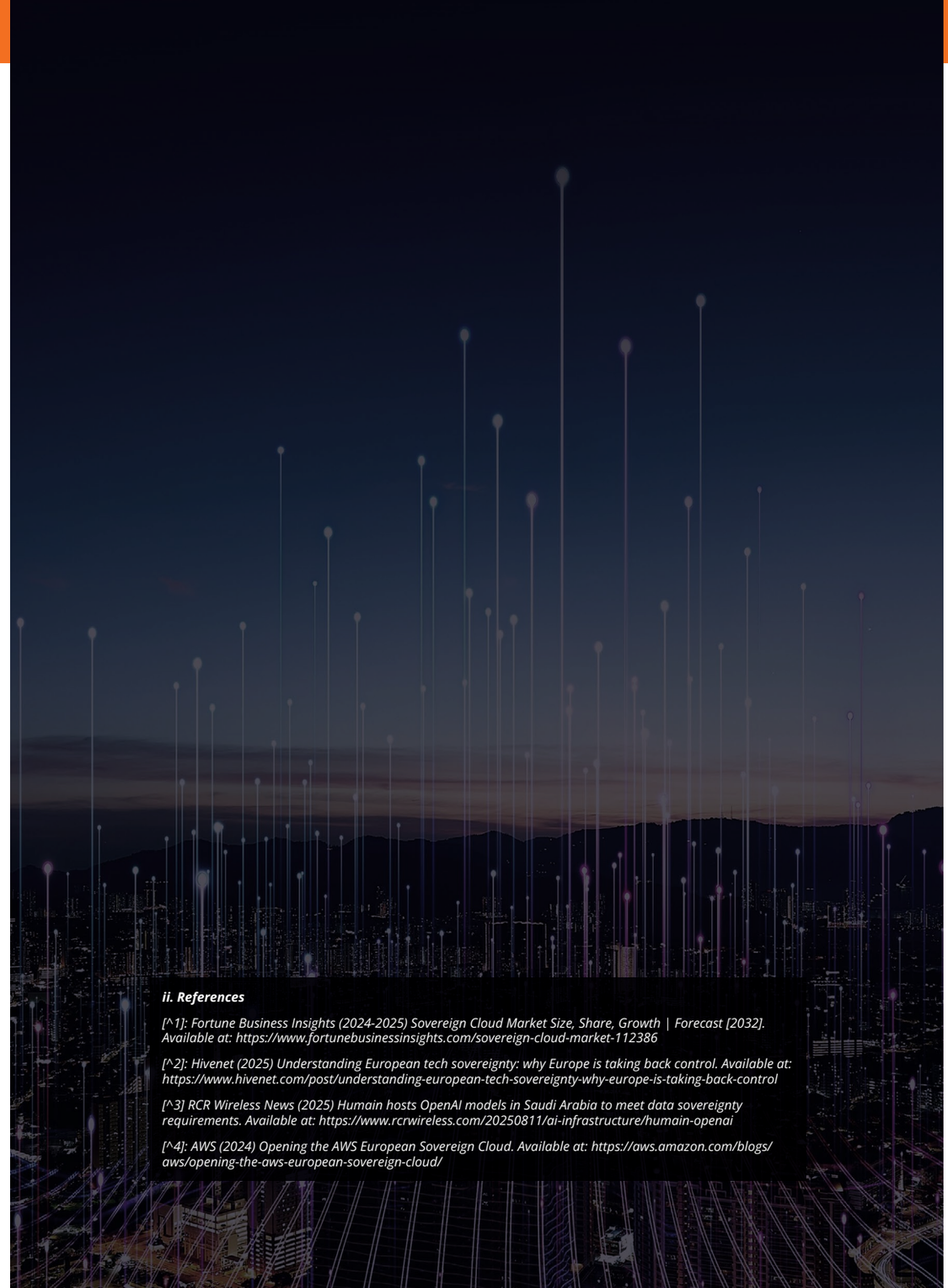
Section 5

CONCLUSION: **BUILDING A SOVEREIGN FUTURE**

Sovereignty spans three interconnected dimensions: digital infrastructure, data control, and AI deployment. Together, these layers enable organisations to maintain strategic autonomy while participating in global digital ecosystems.

Success requires open platforms delivering control without constraint. Openness and portability prevent lock-in, customer-controlled encryption and comprehensive governance safeguard data, and sovereign AI capabilities support auditable, locally governed innovation.

As geopolitical tensions persist, regulations tighten, and AI transforms society, digital sovereignty is no longer optional. Decisions made today will shape competitive position, regulatory resilience, and operational freedom for decades. Organisations that embed sovereignty principles can navigate complexity whilst capturing full value from data and AI.



ii. References

[^1]: Fortune Business Insights (2024-2025) Sovereign Cloud Market Size, Share, Growth | Forecast [2032]. Available at: https://www.fortunebusinessinsights.com/sovereign-cloud-market-112386

[^2]: Hivenet (2025) Understanding European tech sovereignty: why Europe is taking back control. Available at: https://www.hivenet.com/post/understanding-european-tech-sovereignty-why-europe-is-taking-back-control

[^3] RCR Wireless News (2025) Humain hosts OpenAI models in Saudi Arabia to meet data sovereignty requirements. Available at: https://www.rcrwireless.com/20250811/ai-infrastructure/humain-openai

[^4]: AWS (2024) Opening the AWS European Sovereign Cloud. Available at: https://aws.amazon.com/blogs/aws/opening-the-aws-european-sovereign-cloud/