



Global Data Sovereignty Report 2026

Surveying enterprise priorities, adoption,
and organizational readiness



Table of contents

Executive summary

The sovereignty gap

Recognition without readiness

Catalysts of data sovereignty measures

Dependence on one-off measures

Regional and enterprise breakouts

Awareness of data sovereignty failures

Technology trade-offs and AI impact

The procurement shifts

The AI intersection

The execution challenge

Data sovereignty's influence on workloads and investments

Workload trends

Data sovereignty influencing long-term investments and plans

Bridging the sovereignty gap: Operational bottlenecks and skill deficits

Conclusion

3

4

5

5

6

6

6

7

8

9

10

11

11

11

12

13

Executive summary

For over a decade, data has been an enterprise’s most valuable asset.

The emergence of generative artificial intelligence (AI) has only underscored its importance. In parallel, escalating geopolitical instability has elevated the issue of data sovereignty—where data is stored, who can access it, and which legal jurisdictions govern it—from a back-office compliance detail to a key pillar of operational resilience.

To evaluate this shift, Everpure™ commissioned market research firm Vanson Bourne to conduct an independent study of 2,100 enterprise organizations across eight key markets: the UK, France, Germany, Australia, Japan, South Korea, Singapore, and India.

Research scope at a glance

Sample size

2,100 enterprise organizations

Target regions

UK, France, Germany,
Australia, Japan, South Korea,
Singapore, India

Primary focus

Drivers, risk mitigation,
AI impact, and execution
hurdles



The findings

90%

of respondents consider data sovereignty a business concern.

62%

lack full visibility into where their data resides— or who can access, control, and manage it.

64%

of organizations have no formal data sovereignty strategy in place.

56%

lack the internal skills and capacity to deliver data sovereignty initiatives.

The findings reveal a disconnect between priority and readiness across global enterprises.

This report explores the gap between awareness and action, and how global organizations are addressing data sovereignty today.

The sovereignty gap

“ We talk about it [data sovereignty] a lot internally now, but nothing has really changed, to be honest.”

Senior management, banking (3,000–4,999 employees), Germany

62%

have less than full visibility and control into who can access, control, and manage their data.

Recognition without readiness

The survey revealed that the majority of organizations (90%) consider data sovereignty a business concern, but this awareness is not aligned with action.

64%

of respondents have yet to formally embed a data sovereignty strategy, with 38% either still developing capabilities or completely lacking them.

93%

recognize data management¹ as critical or very important to sovereignty, while 62% still lack full visibility into who can access, control, and manage their data.

“Data sovereignty is a priority in the context of widespread geopolitical insecurity and new threats.”

Senior management, technology
(3,000–4,999 employees), France

Catalysts of data sovereignty measures

Organizational action remains focused on immediate tactical measures rather than addressing long-term operational risks.

Reported drivers of data sovereignty action

47%

Cybersecurity risks
(e.g., data breaches, data leakage)

39%

New regulatory and compliance requirements (potential for fines)

34%

AI adoption/rollout of new AI initiatives

26%

Business/service continuity and resilience

25%

Customer trust/reputation risk

19%

Board-level strategic direction

Geopolitical and operational risks receive lower prioritization

26%

identified service disruption risks from global political uncertainty or economic policy.

56%

maintain no mitigation strategy for data exfiltration (geopolitical) or service disruption.

9%

cite protection against foreign government data requests as a top priority.

9%

highlight lowering concentration risk of overseas technology providers as a top priority.

Dependence on one-off measures

Encryption and access controls represent the most widely deployed sovereignty measures (implemented by 60% of respondents), primarily to address the risk of data exfiltration.²

By comparison, measures that safeguard operational continuity against denial of service (DoS)³ are less common, with around half (49%) protecting against DoS through segmenting data and applications by jurisdiction or implementing sovereign or private cloud environments (53%).



Regional and enterprise breakouts



Strategy adoption

Japan has the highest rate of formal strategy implementation (47%), whereas Singapore reports the lowest adoption rate (81% lack formal plans).



Risk prioritization

The UK places the lowest priority on extraterritorial risk; 5% rank protection against foreign government access requests or lowering concentration risk of foreign providers as top priorities.



Enterprise size

45% of large enterprises (5,000+ employees) have formally embedded a sovereignty strategy, compared to 30% of smaller firms (less than 3,000 staff)—12% of these smaller businesses remain completely unaware of sovereignty challenges altogether.

Awareness of data sovereignty failures

91%

state that a data sovereignty failure would result in significant financial or reputational risk.

88%

indicate that it could cost senior decision-makers their jobs.

“ It [data sovereignty] has changed from risk management to board-level strategy. This is viewed as a core capability for preserving customer trust and protecting proprietary algorithms from foreign access.”

Senior management, financial services excluding banking (1,000–2,999 employees), Singapore

2

Technology trade-offs and AI impact

“Vendor evaluations are now more stringent, with a greater emphasis on regional hosting capabilities and sovereignty promises.”

C-level executive, banking (3,000–4,999 employees), UK



The procurement shifts

Established technology norms are being reevaluated in the wake of data sovereignty. Nearly nine in 10 respondents (85%) indicated they would sacrifice access to advanced features and functionality in order to partner with a sovereign cloud provider.

Sovereignty has also rapidly become a baseline criterion in procurement

80%

report that data sovereignty has become more important during vendor selection and RFP processes over the last 12 months.

40%

are actively limiting the use of SaaS platforms that rely on nondomestic hosting infrastructure.

Evolving sovereignty decisions

2%

Prior to 12 months ago: Just 2% say that data sovereignty has been a significant consideration for their organization's vendor selection or RFP processes.

32%

now classify data sovereignty as a significant consideration as part of their vendor selection/RFP processes.

Regional differences in procurement

44%

of organizations in India lead in treating sovereignty as a "significant" consideration when it comes to vendor selection/RFP processes, while Australia is at 16%.

49%

German firms report the highest rate of limiting the use of foreign-hosted SaaS platforms, with 49% taking active measures.

The AI intersection

AI has become a catalyst for data sovereignty initiatives

92%

view data sovereignty as a critical part of their overall AI strategy.

93%

believe sovereign AI capabilities provide a competitive advantage.

87%

will prioritize local or sovereign environments for most/all AI initiatives or workloads that are considered high risk or sensitive in the next one to three years.

Sovereignty's impact on AI

46%

of respondents regard sovereignty as a way to ensure confidence and trust in AI adoption.

45%

agree data sovereignty influences where AI models and data are hosted.

36%

report governance and control of AI models are a high priority in cloud sovereignty evaluations, alongside visibility of and control over data access (39%) and encryption and security controls (39%).

“ My biggest challenges are migrating legacy systems to sovereign clouds without downtime, closing the skill gap in compliance plus cloud tech, and balancing advanced features with data residency needs. Sovereign providers are improving but still lag hyperscalers on some AI tools.”

Senior management, emergency services (5,000+ employees), India

39%

acknowledge that sovereign AI introduces additional operational complexity.



Section

The execution challenge

“Currently, we prioritize storing highly sensitive business data locally in order to improve compliance, strengthen security, and build customer trust.”

Senior management, healthcare—private (1,000–2,999 employees), Japan

Data sovereignty’s influence on workloads and investments

Workload trends

To align with regional compliance requirements, enterprises are rebalancing workloads across global clouds, local infrastructure, and sovereign environments.

1%

Prior to 12 months ago: Only 1% had moved the majority or all of their enterprise data to local/sovereign infrastructure.

28%

Today: 28% have repatriated the majority or all of their data.

41%

One-to-three-year projection: 41% plan to host the majority or all of their data in local or sovereign environments. For sensitive workloads, sovereign hosting is a preferred option: 92% expect local/sovereign clouds to be the default deployment model for sensitive workloads within three years, with 54% saying their data sovereignty initiatives will prioritize high-risk or sensitive AI workloads.

Data sovereignty influencing long-term investments and plans

“There are no ready-made implementation templates. Every step requires trial and error, with high costs associated with mistakes.”

C-level executive, banking (1,000–2,999 employees), Germany

67%

will treat sovereignty as a strategic focus for the next three years, with 29% extending that timeline to five years.

86%

increased their sovereignty investments in the past six to 12 months.

29%

implemented significant budget increases over the last six to 12 months, rising to 42% among firms that have formally embedded data sovereignty into business strategy, and 48% among firms with full visibility of who accesses, controls, and manages their data.

Bridging the sovereignty gap: Operational bottlenecks and skill deficits

Despite rising investments, execution bottlenecks delay implementation.

Primary implementation challenges

57%

struggle to balance sovereignty with wider strategic priorities.

50%

face cost and budget constraints.

56%

lack the internal skills and capacity to deliver data sovereignty initiatives.

36%

experience challenges with executive buy-in.

55%

cannot keep pace with changing regulatory requirements.

19%

report that their data strategy is being driven by the board.

“ Throughout the leadership discussions, the most difficult problem is persuading board members that sovereignty is worth investing in.”

C-level executive, energy (5,000+ employees), South Korea



Conclusion

The 2026 data indicates that while data sovereignty has transitioned into a core strategic priority for major enterprises globally, operational capabilities have not kept pace. While investment in data sovereignty initiatives continues to rise, organizations face challenges across data visibility and management capabilities, talent shortages, and the rollout of holistic and strategic approaches to sovereignty.

“ We face a shortage of skilled professionals with expertise in both data sovereignty regulations and technical implementation.”

Senior management, insurance (5,000+ employees), Australia

Bridging this execution gap will determine whether enterprise organizations can successfully balance international regulatory demands, cloud scalability, and secure AI deployment over the coming decade.

Read the Blog: Sovereignty’s Data Imperative

1 | Data management is the process of collecting, storing, organizing, protecting, and governing organizational data across geographical locations and throughout its life cycle. It ensures data quality, visibility, accessibility, regulatory compliance, and availability for decision-making and business operations.

2 | Data exfiltration in this context is the legally compelled transfer, copying, or extraction of data from a computer system, network, application, or device to an external location, driven by foreign authorities.

3 | DoS in the context of data sovereignty refers to the loss of access to essential digital services arising from extraterritorial legal or political actions that restrict or revoke service, disrupting business operations.

Visit Our Website

