Data Sovereignty: A New Era

Navigating Risk in a Dynamic World

PURESTORAGE®

UTS Institute for Sustainable Futures

Position Brief

This position brief was written by Pure Storage® and informed by research conducted by the University of Technology Sydney with a pulse survey to capture the mood of enterprises on data sovereignty.

Introduction

Over the last 20 years, digital innovations have had a profound impact on our daily lives, while simultaneously driving innovation and transformation for governments and businesses. However, when presidents, prime ministers, and CEOs alike talk about data, it's clear that something different is happening.

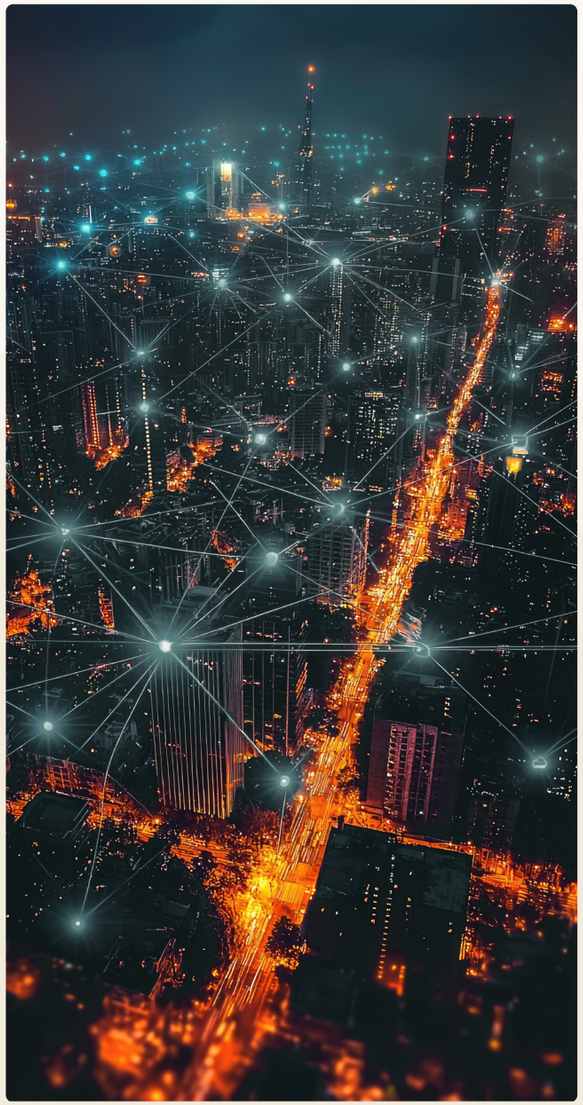
As global geopolitical uncertainty persists, the topic of data sovereignty is top of mind for governments, regulators, and businesses. Defined as the principle that data is subject to the laws and governance structures of the country in which it is collected or stored, data sovereignty is about who has the authority to dictate how data is managed, accessed, and used, particularly in an increasingly interconnected and data-driven world.

> **"Once data is created and stored, ensuring that it's only ever in one place and only ever within a geographic boundary is actually quite a tricky issue."**
>
> DATA GOVERNANCE EXPERT, AUSTRALIA

The likely introduction of regulations and government directives to create sovereign capabilities and the dynamic AI landscape are making the topic of data sovereignty more urgent. This position brief was developed to shine a spotlight on the issue, raise awareness of the risks of inaction on data sovereignty, and stress the urgency for organisations to act in order to mitigate these risks.

To inform this position brief, **Pure Storage** commissioned the **University of Technology Sydney** to capture organisations' views of the data sovereignty landscape. The pulse survey, deployed across nine countries—**Australia, New Zealand**, **India**, **Japan**, **Singapore,** and **South Korea** in Asia Pacific and the **United Kingdom (UK)**, **France**, and **Germany** in Europe—included interviews with a diverse range of experts and practitioners from across industry, the research sector, and data governance leadership.

> **"The real opportunity of data is solving global challenges—from health to food security to climate change. But that requires collaboration, and multilateral cooperation is under strain in today's political climate."**
>
> CEO OF A LARGE FINANCIAL SERVICES FIRM, UNITED KINGDOM



The Risks of Not Dealing with Data Sovereignty

1 Risk: Service Disruption

Today's uncertain geopolitical landscape has introduced a heightened risk of service disruption for organisations that depend on services from non-domestic providers—stressing the importance of considering where data is located and managed and where services originate.

Imagine logging in one morning and discovering that critical, customer-facing services are down. Aside from panic, your first thought might be a cyberattack or an IT failure. The idea that one of your business-critical IT subscription services, whether it's a financial or communication platform, has been cut off by a foreign entity may not enter your thoughts. This is no longer a dystopian scenario, but a potential harsh reality in today's dynamic geopolitical landscape.

We have already seen examples of services being turned off by foreign entities. We have also seen US cloud providers taking concrete steps to protect the cloud deployments of foreign organisations by adding clauses to their contracts to keep services online in the event of a suspension order in court. While this is an example of positive action, it highlights the very real and immediate risk of service disruption.

The effects of service disruption can be severe and impact organisations in many ways. From a regulatory perspective, frameworks such as the EU's Digital Operational Resilience Act (DORA) can now mandate the speed at which organisations must recover from serious digital disruptions, as well as their resilience to downtime in key sectors.

100%

of respondents said data sovereignty risks, including the possibility of service disruption, have caused organisations to consider where their data is located.

Exposure to foreign-led service disruptions will be difficult to mitigate, and the consequences of failing to comply can be high—from loss of customer trust, revenue impact, and reputational damage to monetary fines.

> **"...If you don't control the whole stack, how can you say you have data sovereignty? Even if you're storing your data purely under your legal jurisdiction, but it's stored in a proprietary form, should you lose the access to that software or to that format, how can you assert sovereignty?"**
>
> DATA GOVERNANCE MANAGER, NEW ZEALAND

Implication

The mission criticality of IT service delivery is deeply entwined with the success or failure of any organisation. Data sovereignty further adds to this and poses a clear and present danger for those organisations who do not have plans in place to mitigate such risks.

Continued: **The Risks of Not Dealing with Data Sovereignty**

2 Risk: Foreign Influence

Foreign government access and global surveillance was noted as a risk factor by almost one third of interviewees, who raised ethical, privacy, and national security challenges. Unauthorised access to data, particularly sensitive data such as medical or financial records, can significantly impact public trust in an organisation. Government access to data and broader surveillance activities are important considerations for organisations navigating data sovereignty. The key distinction is between legitimate access, which follows established legal frameworks such as due process and court orders, and illegitimate access, which involves unauthorized or unlawful intrusion by external actors.

Organisations must understand that illegitimate access to sensitive information—such as medical or financial records—not only creates security and compliance risks but also erodes public trust.

Despite the high stakes, substantial dependency on non-domestic cloud service providers, and the growing complexity of managing data across jurisdictions highlight that many boards and leadership teams remain unprepared to evaluate how data could be misused and how to manage reputational fallout if an incident occurs.

> **"Increasingly it's going to be difficult to put data in one of the big players because you won't want to be putting commercially sensitive or private information about customers into an uncertain world. I think we can increasingly see people concerned about the privacy of these models and the sensitivity of sharing information, especially with overseas companies."**
>
> AI EXPERT, AUSTRALIA

Implication

Strong planning for data sovereignty means tackling these risks head-on with clear governance policies, robust technical safeguards, and transparent incident response practices.

3 Risk: Navigating Emerging Legislation and Regulations

Failing to take data sovereignty seriously can have significant regulatory consequences. This applies to regulation that an organisation must comply with as well as regulation that may be used "against" an organisation.

Since 2018, General Data Protection Regulation (GDPR) has been in effect globally to protect EU citizens. GDPR identifies how personal data must be handled and processed, including protecting its integrity, enforcing confidentiality, and providing individuals with rights over their data. Japan's Act on the Protection of Personal Information is generally viewed as an equivalent to GDPR, while in Singapore the Personal Data Protection Act was updated in 2020, bringing it more into alignment with some of the GDPR controls.

What is clear is that more regulation is on the horizon within the EU and further afield. With the European Strategy for Data and the forthcoming Data Union Strategy, we see the foundations for upcoming regulation specifically addressing data sovereignty in the EU.

> **"Regulation is not necessarily a barrier to innovation. Quite the opposite, it's actually a net positive."**
>
> AI EXPERT, AUSTRALIA

Implication

Organisations should prepare for regulatory evolution.

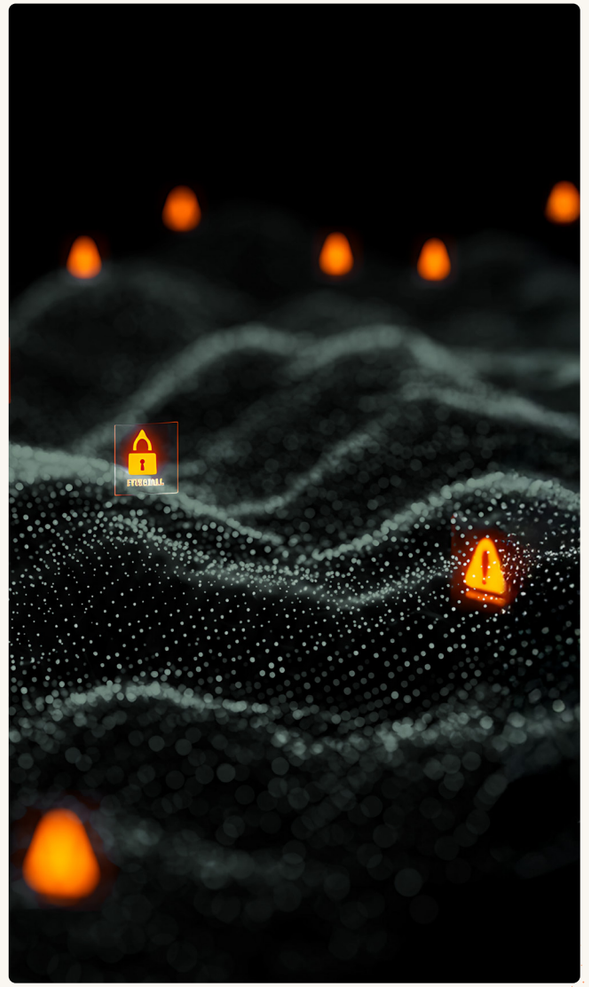
Continued: **The Risks of Not Dealing with Data Sovereignty**

The Impact of Risks

A Perfect Storm

Enterprises operating in sensitive sectors or in regions affected by international tensions are recognising the need to reduce their exposure to infrastructure they can't fully control. Foreign influence over, and access to, sensitive data is a prominent risk to customer/citizen trust and reputation. Not adequately dealing with data sovereignty concerns can lead to brand damage and the loss of customer trust. Combining the threat of service disruption with the associated financial and reputational damage creates a perfect storm. Any company, regardless of industry, that values its ability to maintain business continuity, resilience, and uninterrupted service to customers should be aware of the challenges presented by data sovereignty.

However, it's important to note that the inability to strike a balanced approach to data sovereignty, whether forced down a certain route by regulation or as the result of a sovereign-first strategy, opens organisations up to the risk of losing access to cost-effective, agile or innovative services.



92%

of respondents said not adequately dealing with data sovereignty concerns can lead to reputational damage.

Implication

This finding suggests the marketplace understands the wide-ranging impact that data sovereignty can have on an organisation, extending beyond service delivery and revenue implications to the way an organisation is perceived by its stakeholders.

85%

of respondents said not adequately dealing with data sovereignty concerns would result in loss of customer trust.

Implication

Trust is the very foundation upon which organisations and companies operate, and this finding illustrates that data sovereignty is becoming a defining factor in how our digital society functions.

Challenges to Building Sovereign Capabilities

Geopolitics is shaping where data is stored, how services are delivered, and the supply chains that power advanced technologies. Nations investing in artificial intelligence and other transformative fields rely on secure access to critical components and raw materials. Stable and transparent supply chains are therefore vital for competitiveness and technological sovereignty. At the same time, sustainable approaches to energy must be part of the planning, as sovereign capacity buildouts will incur a substantial demand on power grids.

The semiconductor industry exemplifies the supply chain issue. For example, chip companies rely on advanced manufacturing in Taiwan, which in turn relies on highly engineered extreme ultraviolet (EUV) lithography machines from the Netherlands. EUVs are dependent on critical optical components from Germany, which in turn uses specific raw materials, such as desert sand sourced exclusively from certain regions in Australia. The reality is that no single country possesses all the necessary resources, technologies, and manufacturing capabilities to deliver a modern data centre on its own.

> **"AI is fast becoming a geopolitical force, and data centres are the chess pieces on the board. Decisions about where to build, how to power them, and their environmental impact are increasingly central to global negotiations."**
>
> AI GOVERNANCE LEADER, ASIA

By working together, the global community can ensure technology delivers broad and equitable benefits, rather than being constrained by opaque or exclusionary practices.

It's not only supply chains that need to be scrutinised on the journey to building sovereign capabilities—the global AI race and resulting energy crisis is also critical. The impetus to build sovereign AI capabilities is driving the construction of data centres, which consume

92%

of respondents felt that geopolitics is increasing the risks of not dealing with data sovereignty.

an exorbitant amount of power as well as natural resources, including land and water. Sustainability trade-offs emerge when sovereignty is prioritised. While the construction of sovereign data centres is considered an increasing priority by many nations, data centre energy demands are projected to more than double by 2030, straining resources and putting pressure on the public energy grid.

If data centre growth projections are to be met, organisations and nations will need to prioritise, or even mandate, the most energy efficient underpinning technology infrastructure. The good news is that organisations can begin adopting the most power-efficient data centre technologies today. Solutions that reduce power consumption, cooling, and space requirements so that data centres can scale without collapsing under the weight of their energy demands are essential.

> **"Building local data centres is central to sovereignty—but it comes with trade-offs. While they create jobs, they also put pressure on cities, accelerate urban migration, and risk deepening regional inequities."**
>
> DATA GOVERNANCE MANAGER, NEW ZEALAND

What options do forward-thinking organisations have to navigate these complex data sovereignty risks and challenges?

Implication

It is clear that data sovereignty is an issue; therefore, addressing, rather than ignoring, risks associated with it is critical.

How to Navigate Data Sovereignty

A Practical Guide for Taking Action

There are three ways that organisations can react to data sovereignty:

1 Take a More Intentional Approach to Risk Assessment (Recommended Route)

Define a data strategy that addresses the urgent demands of the situation, determining what data should go where and how it should be managed based on a number of different metrics, such as the sensitivity of the data, nature of personal information, downstream impact, and potential for identification (for example, through metadata). This is a bold approach that requires vision and planning.

2 Take a Conservative Route and Detach From Non-Domestic Public Cloud Service Providers

This is a risky option and likely to set organisations back in achieving their business objectives due to loss of access to innovation and financial fallout.

3 Do Nothing and Hope None of The Risks Catch Up with Them

This is highly risky, and there is no protection from the potentially devastating financial and reputational repercussions of disruptions attached to data sovereignty.

Best Practices for Taking Action

Pure Storage recommends the following for organisations that are going down the first route:

Start with a Risk Assessment

Understanding application landscapes is crucial. Not all data or business applications are a material risk from a sovereignty perspective. This needs to be evaluated from two dimensions: the criticality of the service and the sensitivity of the data. For example, a room booking system may be acceptable in an external cloud environment, but the sovereignty of payroll and critical business services may need to be considered and evaluated against risk.

Consider Hybrid Approaches

Hybrid capabilities allow organisations to keep critical workloads in sovereign hosting environments while leveraging public cloud services for non-sensitive functions—providing both sovereignty and operational flexibility.

Evaluate Sovereign Service Providers

Data centre operators like AUCloud in Australia, Deutsche Telekom and Ionos in Germany, and Beyond.pl in Poland are building regional capabilities, including AI-as-a-service capabilities using foreign technology, but under sovereign control. Multiple deployment options exist, so organisations don't have to build everything themselves. When evaluating a sovereign service provider, organisations should consider:

- **Jurisdictional independence**: Ensure data location, provider ownership, and operational resources are free from foreign influence or legal override mechanisms.
- **Operational resilience**: Evaluate incident response procedures and infrastructure efficiency to ensure sovereignty doesn't compromise availability or performance or increase costs.
- **Compliance and exit planning**: Confirm audit capabilities align with local regulations—DORA, GDPR, and EU AI Act in Europe; Digital Personal Data Protection (DPDP) Act in India; Act on the Protection of Personal Information (APPI) in Japan; and Personal Data Protection Act (PDPA) in Singapore—and that vendor lock-in doesn't prevent data portability.

By asking the right questions, enterprises can ensure that their sovereign service partners enable innovation without compromising control, compliance, or resilience.

> **"AI is certainly redefining the boundaries that we need to think about [in relation to] protecting data and what data sovereignty actually means."**
>
> DATA GOVERNANCE EXPERT, AUSTRALIA

Prepare for Regulatory Evolution

With the EU investing €200 billion in AI infrastructure and the increasing focus on critical national infrastructure, sovereignty requirements are likely to expand. Building or deploying into sovereign infrastructure now positions organisations for future mandates and success.

78%

of respondents said that the different data strategies they are adopting include multiple service providers, sovereign data centres, and embedding data governance requirements in all commercial agreements.

Implication

Organisations are beginning to address issues of data sovereignty, which should act as a wake-up call for those still standing on the sidelines.

Conclusion

What were once considered potential risks from inaction on data sovereignty are now looming realities. Service disruption, foreign government interference, regulatory penalties, and financial/reputational damage are top of mind. Addressing the sovereignty challenge doesn't imply a binary choice between complete disengagement from non-domestic public cloud services or outright disregard for data sovereignty risks. Pure Storage recommends that organisations and their boards take a proactive, intentional approach that starts with a risk assessment of what is important for their business and then adopt a hybrid approach that marries sovereignty with operational flexibility. Without a forward-looking data sovereignty strategy, organisations expose themselves to the severe consequences of their own hesitation. Ultimately, inaction will be measured in a loss of trust, financial damage, technological vulnerability, and irreparable competitive disadvantage. It's time to act in order to safeguard resilience, innovation, and trust in a new era where control over data is set to become a defining battleground for businesses and nations alike.

Methodology

Pure Storage commissioned the University of Technology Sydney to capture organisations' views of the data sovereignty landscape. In-depth interviews were conducted with a diverse range of experts and practitioners, including CEOs, CIOs, and leaders in data, IT, and AI governance, from across industry and the research sector. Interviews were conducted with experts across nine nations. These interviews contributed perspectives that may not always be communicated in public domains. Twenty-two semi-structured interviews were conducted via video communications between July and August 2025 and recorded and transcribed for analysis.

All research activities were approved by the UTS-ISF research ethics program, overseen by the UTS Human Research Ethics Committee (HREC).

About Pure Storage

Pure Storage (NYSE: PSTG) delivers the industry's most advanced data storage platform to store, manage, and protect the world's data at any scale. With Pure Storage, organisations have ultimate simplicity and flexibility, saving time, money, and energy. From AI to archive, Pure Storage delivers a cloud experience with one unified storage as-a-service platform across on-premises, cloud, and hosted environments. Our platform is built on our Evergreen® architecture that evolves with your business—always getting newer and better with zero planned downtime, guaranteed. Our customers are actively increasing their capacity and processing power while significantly reducing their carbon and energy footprint. It's easy to fall in love with Pure Storage, which is why we've received one of the highest Net Promoter Scores in the industry across the years.

For more information, visit www.purestorage.com

www.purestorage.com

ID4255-01-en-09/25