Chapter 1

Global tensions and data regulatory policies

TELEHOUSE

The political rifts and strategic rivalries outlined above are now reshaping routine business decisions. Ongoing conflicts and macro-economic uncertainties must be factored into every tactical or strategic choice.

Access to advanced chips, green energy, and even shipping lanes can be impacted daily with a new sanctions list, or maritime threat, while shifting tariffs can rapidly change every cost-benefit analysis. At the same time, boardrooms that once optimized solely for cost, now have to weigh up questions of national-security alignment, resilience, and the risk that a contract signed today could be outlawed or unaffordable tomorrow.

All these pressures are reshaping the regulatory landscape as governments implement data-flow restrictions, investment screens, and export licenses that dictate where and how companies may operate.

> ***The result is a thickening web of rules that intersects every decision about where to place critical digital infrastructure and makes the choices that data center partners need to make as political as they are technical.***

Stricter data-sovereignty rules and cross-border transfer limits, embodied in frameworks such as the EU's GDPR and China's Cybersecurity Law, are splintering the global regulatory landscape. New US legislation, such as FISA 702 and the CLOUD Act, are also having a significant impact on digital sovereignty worldwide.

Organizations are often now obliged to keep data within each jurisdiction, driving up costs, fostering isolated data pools and preventing them from exploiting the economies of scale offered by international data center platforms.

As sovereignty regimes tighten, regulations are widening their expectations beyond data handling alone. Increasingly, compliance is tied to proof of environmental stewardship, transparent utility planning, and demonstratable community value – all of which now influence whether critical digital infrastructure is approved in a given jurisdiction.

David Chassan, *Chief Strategy Officer at OUTSCALE, Dassault Systèmes, notes:*

"Digital sovereignty is now a design requirement for cloud and AI. Sovereign infrastructure keeps sensitive data and AI workloads under local jurisdiction, protects intellectual property across the model lifecycle, and reduces exposure to extraterritorial constraints. Coupled with secure, energy-efficient data centers, it enables compliant, resilient, and innovative organizations to scale with credible sustainability."

For all these reasons, we are seeing regulatory complexity becoming one of the biggest influences on the evolution of the global data center industry today.

Although business leaders ultimately decide on where to locate their organizations' IT infrastructure, their choices are informed by guidance from data center partners and cloud providers. And the reality is their decisions will be restricted by the ever-tightening rules.

> ***Mandates push in-country hosting; multi-region but jurisdiction-bound designs; strict data residency; edge placement; geo-fencing; segmentation; and pervasive encryption with local peering and cloud on-ramps.***

Bureaucratic hurdles often deepen the challenge. Lengthy licensing and permitting processes, tough investment-screening regimes, and frequently revised foreign-ownership rules can delay projects and inflate budgets.

Meanwhile, export controls and tariffs on core inputs, from advanced chips to fiber-optic cables, turn hardware availability into a day-to-day risk calculation for hyperscale and colocation operators.

> ***These hurdles are already slowing fresh data center investment. Projects can spend months in sequential approvals for land-use, environmental impact, water abstraction, noise, and air permits for large backup-generator farms, followed by grid-connection studies and utility interconnection agreements.***

Separate traffic and heritage assessments often trigger design revisions and resubmissions. On top of this, investment screening adds another layer of timing risk: filings, information requests, and multi-agency coordination can hold up financing and deal close, especially when a campus spans multiple jurisdictions with different thresholds and timelines.

The cumulative effect is delayed ground-break, higher holding costs, and increased contingency in budgets. One indicator of the growing compliance load: a European Commission report from October 2024 found that EU Member States reported handling 1,808 FDI authorisation requests and ex-officio cases in 2023, with 56% proceeding to formal screening, reflecting broader, more active scrutiny that investors must plan around.

At the same time, lengthy licensing and permitting timelines, exacting investment-screening regimes, and shifting foreign-investment rules can delay projects and inflate costs.

Geopolitical trade frictions compound the challenge. Essential equipment: from semiconductors to fiber-optic cable and advanced computing hardware, now sits at the intersection of export controls, industrial policy and supply-chain disruption, turning component availability into a national-security concern.

Geopolitics and national security now shape both data policy and trade. Governments worry about sensitive data held overseas, so rules on cross-border transfers are tightening, even as the EU-U.S. Data Privacy Framework restored a lawful path for transatlantic data flows in July 2023.

European Commission Trade is feeling the same security pull. The United States expanded semiconductor export controls in October 2023, widening restrictions on advanced chips and the tools used to make them. These pressures meet ongoing logistics shocks. UNCTAD reports that disruptions in the Red Sea and major canals pushed container rates sharply higher by mid-2024, complicating planning and lead times.

> ***In terms of geopolitical risk, national security is a key factor. Governments are increasingly concerned about the security of data stored in foreign countries, particularly sensitive information, leading to regulations and policies aimed at controlling data flows and storage.***

So, what's the solution to all these challenges? Business leaders can stay flexible here by treating sovereignty as a design variable.

Region-pinned, modular architectures with data mapping and policy-as-code allow quick rerouting when rules shift. Vendor diversity, neutral interconnection, contracted exit rights, and tested migration playbooks reduce lock-in and keep options open across markets.

Resilience also depends on how easily networks can re-route and scale across multiple interconnection points when conditions change.

Jennifer Holmes, *CEO, The London Internet Exchange (LINX), said:*

"When uncertainty rises, networks prioritize choice and resilience. Rich interconnection ecosystems help keep traffic closer to users, reduce dependency on single routes, and make it easier to adapt when conditions shift."

Data center operators can help by keeping data in-country, choosing certified sites, and building geo-fenced, encrypted networks with local peering and cloud on-ramps. The best providers offer audit-ready facilities, interconnection choices, and sovereign options across key hubs, enabling compliant performance without excess complexity.

Building on that regional approach, operators can open early conversations with regulators, run clear pre-application scoping, and map compliance. They can coordinate parallel design, environmental and security tracks, maintain standard documents and live data rooms, and stage investments. Business customers gain faster approvals, fewer surprises, smoother stakeholder alignment, and lower delay, cost, and risk as a direct result.

Data centers can also assist businesses in navigating geopolitical risks by helping firms plot a course through these rules and disruptions by keeping sensitive workloads within required jurisdictions and supporting low-latency “control towers” for end-to-end visibility.

Supply chains that adapt as conditions shift are equally key. Digital, flexible networks that diversify sourcing and sustain readiness handle shocks more smoothly. Progress tends to come from simpler customs, investment in ports, and rail and wider trusted-trader use.

Incentives for dual sourcing, nearshoring, and smarter inventory create buffers, while common standards and protected data flows reduce friction. During crises, green lanes keep goods moving. Shared visibility tools, supplier support, and workforce programs add capacity. Large companies keep asking for clear rules, faster permits, reliable energy, aligned cybersecurity, and affordable finance for smaller suppliers.