New Kiteworks Report Reveals Organisations Across Every Region Are Spending Millions on Data Sovereignty Compliance

One in three organisations experienced a data sovereignty incident last year.

SAN MATEO, CA, UNITED STATES, February 26, 2026 /EINPresswire.com/ -- Kiteworks, which empowers organisations to effectively manage risk in every send, share, receive, and use of private data, today released its 2026 Data Security and Compliance Risk: Data Sovereignty Report, a cross-regional survey of risk management, compliance, IT, and security professionals that reveals a striking data sovereignty disconnect. Organisations know the sovereignty rules better than ever, but one in three still experienced a sovereignty-related incident in the past 12 months. The report surveyed professionals across Canada, the Middle East, and Europe, covering compliance with PIPEDA, PDPL, GDPR, and emerging AI governance frameworks.

> Regulators, customers, and procurement teams now want proof: who can access the data, who controls the keys, and can you demonstrate compliance on demand."
>
> *Dario Perfettibile, GM of EMEA GTM & Customer Operations, Kiteworks*

The report's most striking finding is the convergence of awareness and the persistence of incidents. Approximately 44% of respondents in each region describe themselves as "very well informed" about data sovereignty requirements—Canada at 44%, the Middle East at 44%, Europe at 44%. Yet incident rates range from 23% in Canada to 32% in Europe to 44% in the Middle East. The most common incident types include data breaches with sovereignty implications (17%), third-party compliance failures (17%), regulatory investigations (15%), unauthorised cross-border transfers (12%), and government data access requests (10%).

"Organisations across every region we surveyed are spending millions on sovereignty compliance, scoring high on awareness, and still getting hit by breaches, unauthorised transfers, and government access requests," said Dario Perfettibile, EMEA GM of GTM and Customer Operations at Kiteworks. "The gap is not knowledge. It's the distance between policy documents and architecture that actually enforces residency, controls access, and produces audit-ready evidence on demand."

Key Findings: The Sovereignty Gap Is Operational, Not Informational

The report reveals several regional dynamics that challenge conventional assumptions about sovereignty maturity. The Middle East reports the highest incident rate (44%) despite 93% of respondents saying PDPL and SDAIA regulations directly impact operations and two-thirds spending over $1 million annually. Canada's 23% incident rate is the lowest, but 40% of Canadian respondents identify changes to Canada–U.S. data sharing as their top concern and 21% flag the U.S. CLOUD Act as a direct sovereignty threat.

In Europe, 44% cite provider sovereignty guarantees as their top barrier to cloud adoption—the highest of any region—despite near-universal GDPR compliance. Notably, environments such as Microsoft GCC High, whilst meeting jurisdictional residency requirements, do not deliver sole encryption key ownership—meaning the provider retains the technical ability to access customer data, a gap that undermines the sovereignty guarantees many organisations require.

Technical infrastructure changes (59%) and legal and compliance expertise (53%) lead the resource drain list, and the majority of organisations spend more than $1 million annually on sovereignty compliance. Yet the report shows the market is shifting from policy to architecture: Compliance automation and enhanced technical controls lead two-year planning strategies across all three regions.

AI Governance Emerges as the Next Sovereignty Battleground
The report also surfaces a growing AI data sovereignty challenge. Roughly one-third of respondents keep all AI training data within their home region, another third use a mixed approach based on sensitivity, and 21% are still developing their AI sovereignty policy. With the EU AI Act now in effect and SDAIA actively shaping AI governance in Saudi Arabia, the report identifies that last group as heading into enforcement cycles without a plan.

Kiteworks' Private Data Network addresses these challenges through capabilities designed for provable sovereignty:

- Sole Encryption Key Ownership: Kiteworks retains encryption key custody within the customer's environment, ensuring the provider is technically unable to decrypt content—even under legal compulsion. For the 10% of respondents who cited government data access requests as a sovereignty incident, this is the architectural difference between a workflow problem and a cryptographic impossibility.
- Flexible Jurisdictional Deployment: On-premises, private cloud, hybrid, and FedRAMP deployment options allow organisations to store sensitive content exclusively within their home jurisdiction—whether Canada, the Middle East, or the EU—with geofencing enforced through configurable IP controls.
- Immutable Audit Trails and Automated Compliance Reporting: Centralised, immutable logs and preconfigured templates for GDPR, PIPEDA, PDPL, DORA, and NIS 2 produce the exportable evidence the report identifies as the critical gap between stated compliance and provable control.
- Unified Data Exchange Governance: Email, file sharing, managed file transfer, SFTP, and web

forms—the channels where third-party failures and cross-border transfer incidents concentrate—are consolidated under a single zero-trust platform.

“Sovereignty used to mean geography—keep the data in the right country and you’re covered,” said Dario Perfettibile, EMEA GM of GTM and Customer Operations at Kiteworks. “That era is over. Regulators, customers, and procurement teams now want proof: who can access the data, who controls the keys, and can you demonstrate compliance on demand. The organisations that build that proof into their architecture will pull ahead. Everyone else will keep knowing the rules and keep getting hit.”

About Kiteworks
Kiteworks enables organisations to manage risk effectively across every send, share, receipt, and use of private data. The Kiteworks platform provides customers with a Private Data Network that delivers data governance, compliance, and protection. It unifies, tracks, controls, and secures sensitive data moving within, into, and out of an organisation, significantly improving risk management and ensuring regulatory compliance across all private data exchanges. With EMEA regional offices in Regensburg, Amsterdam, and Zurich, Kiteworks protects more than 100 million end-users and thousands of enterprises and government agencies globally, including across Europe, the Middle East, and Africa.

Martin Brindley
Martin Brindley PR Ltd
martin.brindley@kiteworks.com
Visit us on social media:
LinkedIn
Facebook
YouTube
X
