Kiteworks

EXECUTIVE SUMMARY

2026 Data Security and Compliance Risk: Data Sovereignty in Europe

The Most Regulated Market in the World Is Still Learning That Contracts Can't Override Laws — and Architecture Is the Real Defence

Europe has the most mature data sovereignty ecosystem on the planet. **GDPR set the global standard. NIS 2 and DORA are tightening operational resilience requirements. The Data Act took effect in September 2025, and the EU AI Act's GPAI obligations followed in August 2025.** European organisations report the highest combined understanding of any region surveyed — 80% describe themselves as "well" or "very well" informed about sovereignty requirements.

But maturity has not eliminated risk. One in three European respondents experienced a sovereignty-related incident in the past 12 months. The provider trust problem persists: 44% cite concerns over provider sovereignty guarantees as a barrier to adopting European cloud solutions. And geopolitical shifts — particularly U.S. policy changes — are adding new urgency to questions that the Schrems II decision was supposed to have settled years ago. This summary distills the key European findings from a cross-regional survey spanning Canada, the Middle East, and Europe.

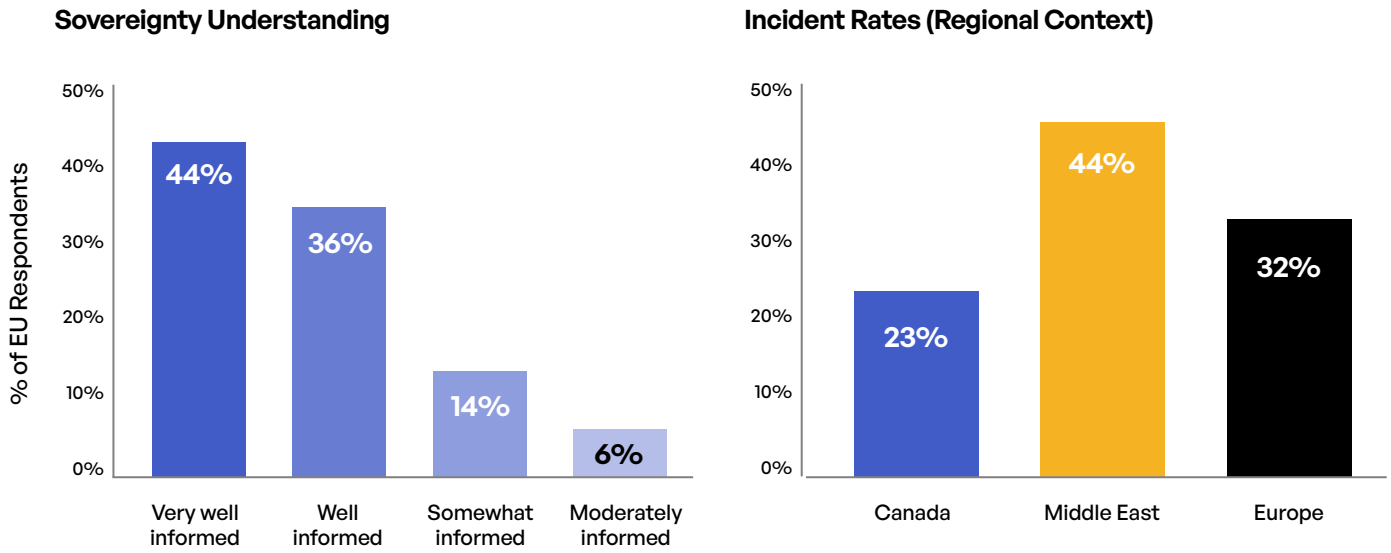
44% **of European respondents cite concerns over provider sovereignty guarantees as a barrier — the highest of any region, and a direct challenge to the "just use EU data centers" assumption**

Regulatory Maturity Hasn't Closed the Incident Gap

European sovereignty understanding is strong and broad-based. 44% say they are "very well informed," 36% "well informed," with only 6% at the lowest tier. **GDPR compliance is near-universal. NIS 2 and DORA readiness are well advanced, with most organisations in the "implementation phase" or "mostly compliant" category**.

Yet 32% of European respondents experienced a sovereignty incident in the past year — higher than Canada's 23%, though below the Middle East's 44%. The most common incident types are unauthorised cross-border transfers, regulatory investigations, data breaches with sovereignty implications, and third-party compliance failures. The message is clear: Regulatory maturity reduces but does not eliminate incidents. The remaining gap is operational, not informational — and closing it requires architecture, not more awareness training.

Europe's Regulatory Maturity Hasn't Eliminated Incidents — One in Three Stills Reports One



Sovereignty understanding among European respondents (left) and incident rates in regional context (right)

The Business Case: Sovereignty as a European Competitive Edge

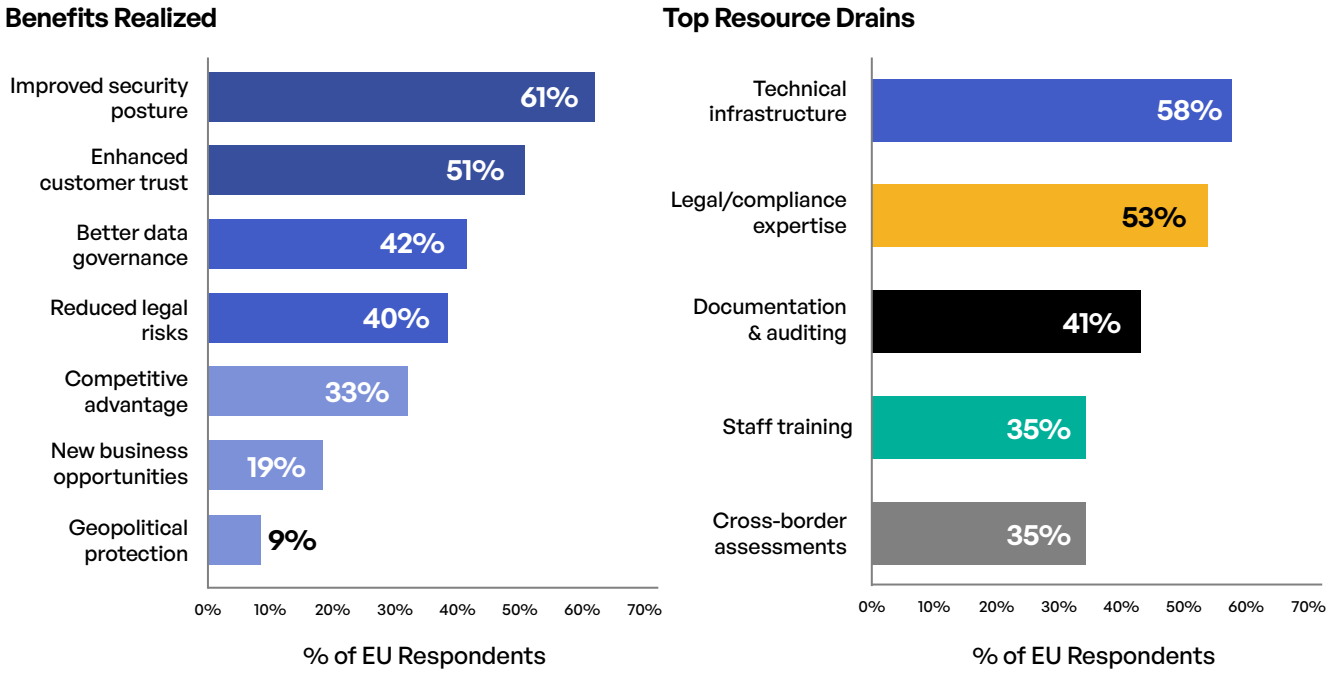
European respondents associate sovereignty with tangible business value. **Improved security posture leads at 61%, followed by enhanced customer trust (51%), better data governance (42%), reduced legal risks (40%), and competitive advantage (33%).** These numbers position sovereignty not as a regulatory burden but as a market differentiator in Europe's regulation-conscious business environment.

The Provider Trust Deficit Is Europe's Defining Sovereignty Challenge

Forty-four percent of respondents flag concerns about whether their cloud providers can genuinely guarantee sovereignty. Admissions from major U.S.-headquartered providers about data access limitations have made this more than a theoretical concern. The Schrems II decision established that contracts cannot override foreign government access laws. The implication is structural: European organisations cannot outsource sovereignty to a provider's promise. They need architecture-level controls — encryption key custody retained in-jurisdiction, access policies enforced at the infrastructure layer, and audit trails that prove where data resides and who touched it.

The resource demands, however, are substantial. Technical infrastructure changes lead at 58%, followed by legal and compliance expertise (53%) and documentation and auditing (41%). On spending, 28% of European respondents report annual sovereignty budgets exceeding €5 million, and another 31% spend €1–€5 million. Among organisations with more than 10,000 employees, over 70% fall into these top spending tiers. The investments are concentrated in areas that produce provable control: data residency enforcement, encryption key custody, access policy automation, and exportable audit trails that satisfy both regulators and enterprise customers.

Sovereignty Delivers Clear Business Value — At Significant Ongoing Cost



Business benefits realised from sovereignty compliance (left) and top resource demands (right)

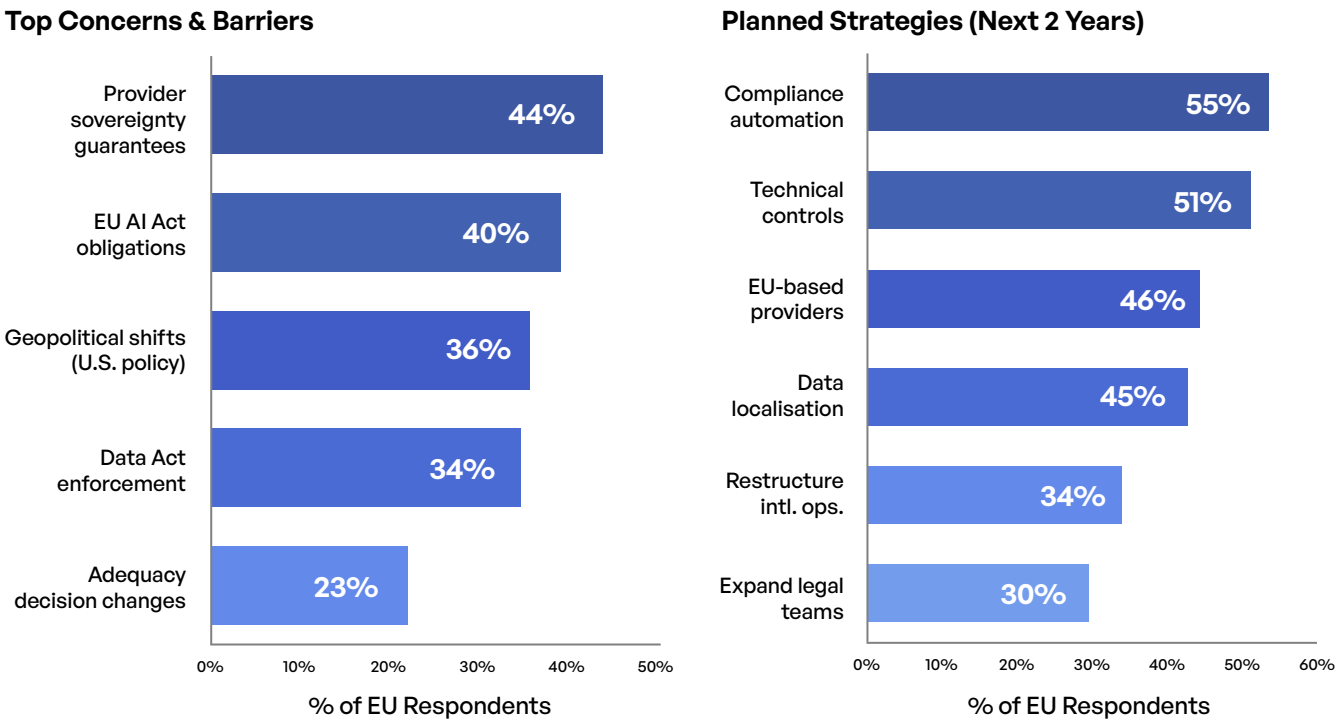
The cost-benefit equation favors organisations that treat sovereignty as an ongoing operating discipline rather than a one-time compliance project. Automation is the efficiency lever — 55% plan to invest in compliance automation over the next two years, making it the top planned strategy across the region.

The Threat Landscape: Layered Regulation Meets Provider Uncertainty

Europe's sovereignty concern profile is uniquely complex because it is layered. **Provider sovereignty guarantees (44%), the EU AI Act (40%), U.S. policy shifts (36%), Data Act compliance (34%), and potential adequacy decision changes (23%) all demand attention simultaneously.** No other region faces this many concurrent regulatory fronts.

The planning response reflects this complexity. Compliance automation leads at 55%, followed by enhanced technical controls (51%), migration to EU-based providers (46%), data localisation (45%), international operations restructuring (34%), and legal team expansion (30%). European organisations are not responding to a single threat — they are building layered defences to match layered regulation. The organisations that succeed will be those that build sovereignty into their architecture rather than bolting it onto existing infrastructure through policy alone.

Provider Trust Regulatory Layering Define Europe's Sovereignty Agenda



Top concerns and barriers (left) and planned sovereignty strategies for the next two years (right)

AI Governance: Preparing for the AI Act Under Sovereignty Constraints

34% of European respondents keep all AI training data within the EU, and another 34% use a mixed approach based on data sensitivity. Safeguard adoption is robust: regular AI audits lead, followed by impact assessments for high-risk AI (48%), transparency documentation, consent management, and bias testing.

The EU AI Act's GPAI obligations, which took effect in August 2025, have formalised what many organisations are already building. But the 34% using a mixed approach need to tighten their sensitivity classifications now that enforcement is underway — "based on sensitivity" is not a defensible standard if the classification criteria are not documented and auditable. Organisations should ensure AI data governance is integrated into their broader sovereignty evidence framework, with the same audit-ready documentation they maintain for GDPR.

Sovereignty You Can Prove: The European Standard

European regulators increasingly require evidence, not assurances. The shift is from "we believe we're compliant" to "we can demonstrate where data resides, how access is governed, and how cross-border movement is prevented or documented." This demands three things. Controls: residency enforcement, encryption key custody, and access policies that prevent unauthorised cross-border movement at the architecture level. Evidence artifacts: exportable audit trails, data residency logs, and compliance reporting that satisfy regulators and customers on demand. Response readiness: tested playbooks for government data access requests, third-party vendor failures, Transfer Impact Assessments, and Schrems II compliance scenarios. Organisations that operationalise all three turn regulatory complexity into a defensible competitive position.

Five Priorities for 2026

1. Close the provider trust gap with architecture, not contracts

44% flag provider guarantee concerns. The response is not better vendor assurances — it's encryption key custody retained in-jurisdiction, access controls enforced at the infrastructure level, and verifiable data residency. Contracts can't override laws; architecture can enforce them.

2. Invest in compliance automation to manage regulatory layering

55% plan this already. With the Data Act and AI Act now in effect alongside NIS 2 and DORA, manual compliance is unsustainable. Automation reduces the 58% technical burden while maintaining the audit-ready evidence regulators demand.

3. Prepare for AI Act GPAI obligations now

40% cite the AI Act as a top concern. Organisations that localised AI training data and implemented regular audits before enforcement are ahead. Those still developing their AI data policy are already behind.

4. Build and test Schrems II and government access response playbooks

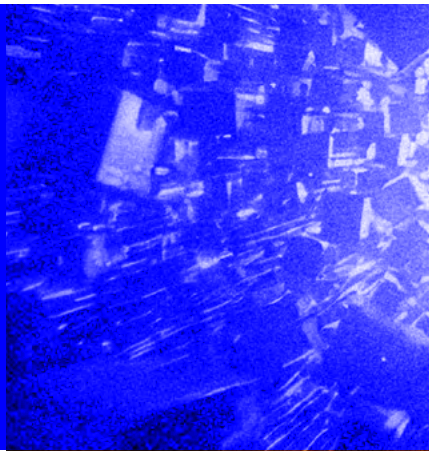
36% cite geopolitical shifts as a concern. Transfer Impact Assessments need to be current, DPF/SCC reliance needs to be documented, and incident response for cross-border transfer events needs to be rehearsed — not just planned.

5. Turn sovereignty into a customer-facing trust asset

51% cite enhanced trust as a benefit and 33% cite competitive advantage. In Europe's regulation-conscious market, the ability to demonstrate sovereignty on demand — through exportable evidence, not policy documents — is becoming a prerequisite for enterprise procurement.

Kiteworks and Data Sovereignty

This report identifies provider trust as Europe's defining sovereignty challenge — 44% of respondents flag concerns about whether their cloud providers can genuinely guarantee sovereignty, and the Schrems II decision confirmed that contracts cannot override foreign government access laws. The Kiteworks Private Data Network is built to close that gap. Its deployment options — on-premises, private cloud, hybrid, and single-tenant hosted — allow organisations to store sensitive content exclusively within EU infrastructure, independent of U.S.-headquartered providers subject to the CLOUD Act.



Kiteworks retains encryption key custody in-jurisdiction, enforces geofencing through configurable IP controls, and applies zero-trust architecture across every communication channel: email, file sharing, managed file transfer, SFTP, and data forms.

For a market where the Data Act, AI Act, NIS 2, and DORA are all now in effect simultaneously, Kiteworks delivers unified compliance controls through centralised audit logs, automated reporting, and preconfigured templates for GDPR, DORA, NIS 2, and PCI DSS. Its immutable audit trails provide the exportable evidence this report identifies as the shift from “we believe we’re compliant” to “we can demonstrate where data resides, how access is governed, and how cross-border movement is prevented.” In Europe’s regulation-layered environment, that evidence capability is what turns sovereignty from a compliance burden into a defensible competitive position.

For the complete report with detailed methodology, industry breakdowns, and regional analysis, download it now.

Download the Report

Kiteworks