INFO-TECH

Digital sovereignty reshapes government tech choices as nations cut reliance on US platforms

On Tuesday, France said it will replace American platforms like Zoom and Microsoft Teams with its domestic video-conferencing tool Visio across all government departments by 2027, citing security concerns and a broader strategy to reduce reliance on foreign software vendors

By Sanjana B

Updated - January 30, 2026 at 09:04 PM.

Governments across major economies are accelerating a shift away from U.S. technology firms, reframing video conferencing and email systems, among others, as critical national infrastructure rising security, data sovereignty and geopolitical risks.

On Tuesday, France said it will replace American platforms like Zoom and Microsoft Teams with its domestic video-conferencing tool Visio across all government departments by 2027, citing security concerns and a broader strategy to reduce reliance on foreign software vendors.

India, meanwhile, is upgrading its legacy government email system to a secure, cloud-based and scalable platform through Zoho to enforce stringent security standards, including end-to-end encryption.

Other countries taking similar steps include the Netherlands, which has approved motions urging the government to reduce reliance on U.S. software firms, including by developing cloud services under Dutch control, and Germany, which is promoting European-built solutions that ensure security, performance and full data sovereignty under European standards.

Germany's Schleswig-Holstein state cut ties with Microsoft, with civil servants, judges and police moving away from tools such as Teams, Word, Excel and Outlook, citing the need for digital sovereignty and reduced reliance on U.S. tech giants.

"Secure communication has crossed the threshold from productivity tool to critical national infrastructure. Governments now design digital systems assuming long-term surveillance, supply-chain infiltration, and nation-state adversaries as baseline threats. Post-pandemic, video conferencing carries cabinet decisions, defence coordination, and diplomatic negotiations," said Sudiptaa Paul Choudhury, CMO, QNu Labs.

Geopolitics is the accelerant, making risks impossible to ignore. At its core, governments demand certainty over where data resides, who controls encryption keys, and which legal systems govern access.

Alongside video conferencing platforms, among others, are increasingly embedding AI-driven capabilities such as visual, speech, and behavioural analytics. They are processing far more sensitive data than earlier generations of communication tools. This shift has prompted governments worldwide to re-evaluate issues of data privacy, processing control, and AI governance, according to Akash Karnik, Global COO, 1Point1 Solutions.

Governments are increasingly factoring in where data resides, how it is processed and who ultimately controls AI models alongside traditional compliance requirements.

“From a data governance perspective, the primary risks stem from limited visibility and control over how sensitive video, audio, and metadata are stored, processed, or used to train AI models outside national jurisdictions. Cross-border data flows complicate compliance with local data protection laws, audit requirements, and enforcement mechanisms, while also raising concerns around third-party access, secondary data use, model reuse and long-term retention. When data storage or AI model training takes place beyond national borders, jurisdictional authority and enforceability weaken, making accountability harder to establish,” he said, adding that for governments, this erosion of control directly impacts trust and transparency when adopting AI-enabled communication platforms at scale.

Indigenous platforms differ from negotiating with foreign vendors, allowing governments to define and enforce their own trust boundaries. Countries own the security architecture, control cryptographic key lifecycles, conduct unfettered system audits and integrate with national identity and security frameworks.

As a sovereign technology export market emerges, nations with advanced indigenous platforms will supply similarly positioned countries seeking alternatives to US-China tech dominance.

This wave is already evident, with countries like Brazil, Indonesia, South Korea and the UAE developing sovereign communication infrastructure. This will only accelerate because data sovereignty is shifting from a policy aspiration to a technical procurement requirement.

Three forces are accelerating the shift: compressed quantum threat timelines, with cryptographically relevant quantum computers now seen as 1–5 years away; regulatory normalisation, as frameworks such as Europe’s GDPR, France’s digital sovereignty mandates and India’s Digital Personal Data Protection (DPDP) Act make data sovereignty non-optional; and demonstrated viability, with France’s Visio rollout showing indigenous platforms can operate at scale.

Karnik highlighted that domestically built platforms can scale to meet enterprise and government requirements, particularly when designed with security, compliance, and data localisation at the core. To become globally competitive, indigenous platforms must combine a trust-led foundation with robust engineering, interoperability, and ecosystem partnerships, enabling cross-market expansion while retaining control over data and AI models.

“Government environments prioritise assurance, auditability, and resilience over consumer collaboration features. Indigenous platforms leapfrog foreign counterparts because of security sophistication. Zoom and Teams retrofit security onto commercial-first architectures; purpose-built sovereign platforms architect security-first. France, Singapore, and India have deployed quantum-safe networks; The EU

and Singapore have set up testbeds to welcome global quantum-tech players to integrate their offerings, ensuring greater flexibility with the right portion of control. India's DRDO collaborations are already deploying video conferencing with quantum key distribution – a technology that no US commercial platform offers because their threat model doesn't demand it. Indigenous doesn't mean inferior; it means optimised for actual government threat models, not shareholder quarterly targets," Choudhury said.

COMMENTS

Published on January 30, 2026