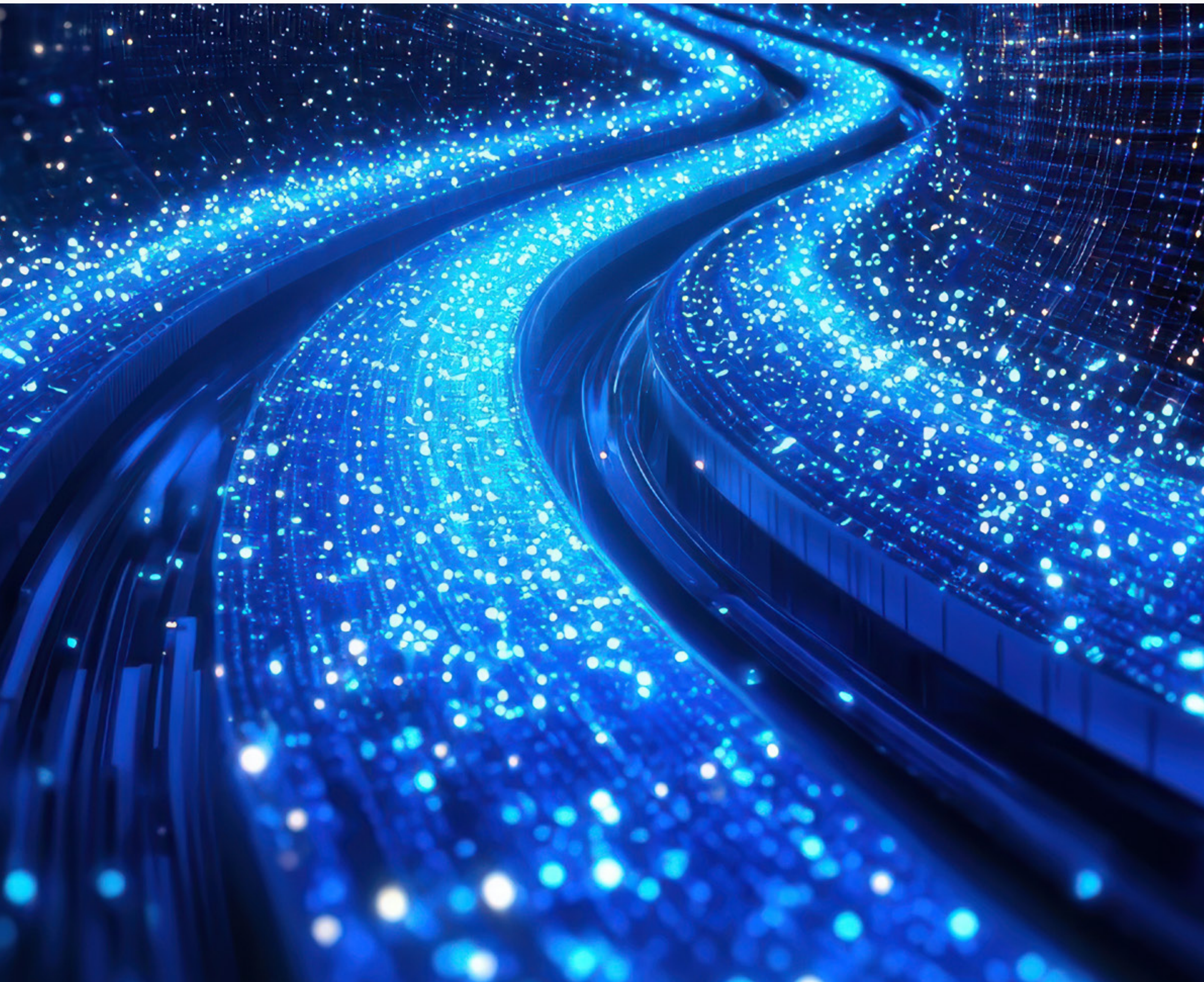
maplewave

WHEN SOVEREIGNTY & SAAS COLLIDE:

Why Digital Contracts Need a New Approach



Executive Summary

Telecom operators have spent the last decade removing paper from their operations and investing in digital contract solutions. Most have met this need by adopting global SaaS e-signature tools that were fast to deploy, easy to scale, and familiar to business stakeholders.

But in today's turbulent world, data sovereignty concerns have telcos re-considering how sensitive contract data is collected, processed, and stored. It's clear that foreign control of critical digital contract platforms is fast becoming a strategic risk, not just an IT detail.

As sovereignty spurs new deployment models, licensing options are similarly under the microscope. Traditional SaaS pricing – per user, per envelope, plus overage fees – are effectively a "success tax" for high volume environments. As telcos transition to on-prem or private cloud deployments, unlimited pricing models are quickly becoming the norm.

In this whitepaper, we will explore:

- How geopolitics has led to the rise of data sovereignty, and why data residency approaches aren't enough.
- Why traditional SaaS models are no longer the best fit for digital contracts.
- The preferred deployment models for telcos who want to future proof their digital contract stack.

01 The Need For Data Sovereignty In A Tumultuous World

When a ‘nice to have’ becomes essential.

“We are in the midst of a rupture, not a transition”.

In his **2026 World Economic Forum speech**, Canadian Prime Minister, Mark Carney, eloquently described how we are witnessing the death of the status quo. There is no mistaking it - the world order is changing. As geopolitical tensions ignite, and old alliances fall, possibilities that would have at one time been considered outlandish are now, shockingly, top of mind.

This global falling-out is impacting everything – including the way we do business, and how we approach problems that we thought were long solved. Fears of government over-reach are driving data sovereignty conversations around the world.

Data Residency vs Sovereignty

Data sovereignty is the principle that digital data remains under the legal authority and control of the country or region where it is created. In other words, all data is subject to the laws of the jurisdiction where it’s created, processed, and stored.

That sounds straightforward when you picture sensitive data sitting on servers in a company owned data centre; you know where the machine is, you know which courts have authority, and you know who holds the keys. For a long time, that was enough. The organization owned or leased the hardware, ran the software, and could point to a physical rack and say, “Our data lives there, under our laws.”

The rise of SaaS (Software as a Service) and the push to move everything to “the cloud” blurred those lines. Instead of running software on their own infrastructure, organizations increasingly subscribe to applications operated by third party vendors, often headquartered in other countries and built on global hyperscale cloud platforms.

To respond to residency concerns, SaaS providers introduced regional and in country “nodes” - instances hosted in specific geographies that could truthfully claim local storage for customer data. For a while, this appeared to solve the problem: if the solution was “EU hosted” or “in country,” many buyers were satisfied.

Three shifts have changed this approach:

- **Geopolitics:** Conflicts, sanctions, and extraterritorial laws like the U.S. CLOUD Act have shown that foreign governments can and do assert authority over data and systems operated by companies under their jurisdiction, regardless of physical hosting location.
- **Cybersecurity Concerns:** Major breaches, ransomware, and supply chain attacks have forced boards to examine not just their own defenses, but the entire ecosystem of providers who hold sensitive data and operational keys.
- **Changing Regulations:** Sovereign cloud strategies, localization mandates, and sector specific rules increasingly single out critical digital infrastructure – including telecoms and trust services – as areas where foreign control is a problem in itself.

In this context, data residency - where data is stored - addresses only part of the risk. Data sovereignty goes further and asks whose laws apply to that data, who can compel access to it, and who actually controls the infrastructure and encryption keys.

A SaaS platform may store documents in a local data centre, but if the vendor is subject to foreign legislation, or if the underlying cloud provider sits in another jurisdiction, then foreign authorities can still assert rights over that data. Similarly, if the vendor controls the keys, the logs, and the operational run book, the customer's ability to enforce its own policies is limited, regardless of where the servers are physically located.

In short, "hosted locally" does not always mean "governed locally." As geopolitical tensions rise and cybersecurity becomes a board level issue, the conversation is shifting from "Is our data in the right region?" to "Whose laws and whose keys ultimately control our most sensitive data?".

Sovereignty increasingly means favouring an organization's own, local, or otherwise trusted infrastructure – including on premise and sovereign cloud models – rather than relying blindly on third party, public, or foreign controlled clouds that only meet the minimum bar of regional hosting.

Evolving Risk Appetites

According to Mimecast, **87% of organizations—and 93% of large enterprises—now factor geopolitics and data sovereignty into cybersecurity vendor selection**, making sovereignty a de facto dealbreaker in many RFPs.

Analysts have framed 2026 as **the year of the cloud exit strategy**, where organizations selectively pull critical workloads out of SaaS/public cloud into private or sovereign environments to reduce exposure to extraterritorial laws and hyperscaler control.

In January 2026, France announced they would **ban public officials from using American video conferencing platforms**, including Google Meet, Zoom, and Teams. The move will ensure the confidentiality of meeting notes and electronic communications by blocking access to AI LLMs, like Gemini. This is a direct response to the CLOUD Act. France will instead move to a domestic option, Visio, by 2027.

Global Sovereignty Spotlight

Below are some key regions and countries, and how they are approaching sovereignty regulations today. This is helpful in understanding where full sovereignty – not just local hosting – is essential.

Region / Country	Sovereignty Posture	Key Themes	Implication for Telco Digital Contracts
European Union	High	• Strong privacy (GDPR) and trust services (eIDAS). • Political sensitivity on third country access.	• Expect EU controlled clouds or on prem for public sector / critical workloads. • Generic US SaaS increasingly unwelcome. • Significant GDPR fines.
China	High	• Strict localization requirements. • Broad "critical data" definition. • Strong national security priority.	• Contracts and identity data must sit on China based, China governed platforms. • Foreign SaaS effectively excluded. • Strong, discretionary enforcement.
India	High	• Rapid localization. • Strong personal protection and sector rules. • Emerging AI storage expectations.	• Telcos serving BFSI/government will need in country contract platforms. • Non local SaaS faces rising friction.
Middle East / GCC	High	• National clouds, egov focus. gov focus • Telcos operate as cloud providers. • Security driven procurement.	• Government/strategic contracts expected on national or sovereign clouds, often operated by telcos themselves. • Rising regulatory scrutiny in key GCC states.
Canada	Medium -High	• Concern over CLOUD Act. • Digital sovereignty framework. • Stricter Quebec rules.	• Canadian owned/on prem or private cloud preferred for gov/regulated sectors. • "Hosted in Canada by US SaaS" under doubt.
CALA (Caribbean & LATAM)	Medium -High	• GDPR inspired privacy laws. • Strong individual rights and rising fines. • Generally liberal cross border rules; sector add ons for telecom and finance.	• Contract repositories and logs can sit in country or in region but must have clear controls on cross border access and operator owned keys. • Foreign or multi tenant SaaS acceptable only with strong DPAs, transfer safeguards, and full auditability. • Workflows must reflect local e-signature tiers and consumer rights rules in key CALA markets.
United Kingdom	Medium	• No general localization mandate. • Adequacy uncertainty with EU. • Critical infrastructure focus.	• Hybrid UK/EU setups. • Sensitive contracts may need sovereign or on prem options to hedge against adequacy changes.
Australia	Medium	• No strict national localization law. • Preference for certified domestic providers in critical sectors.	• Gov and critical infra contracts expected on Australian hosted or sovereign cloud. • Offshore SaaS harder to justify.

02 Digital Contracts: When SaaS & Sovereignty Don’t Mix

SaaS contract are firmly in the crosshairs of sovereignty regulators and financial teams alike.

The benefits of digital contracts are clear - they bring incredible efficiencies, cost savings, and environmental benefits. But most digital contract providers still operate on a pure SaaS model, raising concerns around data sovereignty and unpredictable pricing.

Why Sovereignty Bites Harder For Digital Contracts

Digital contracts are prime targets for data sovereignty; they are full of personal information, sensitive operational details, and act as legal evidence. Unlike generic CRM or analytics tools, contract systems sit at the intersection of PII, commercial secrets, and regulatory workflows. When sovereignty fails here, it is not just an IT issue - it affects disputes, audits, and even eligibility for major RFPs.

The “Success Tax” of Traditional SaaS Pricing

It’s not just data sovereignty that makes SaaS solutions ill-fit for digital contract solutions. Their pricing structure itself increasingly clashes with telecom realities.

E-signature SaaS solutions are usually priced based on usage: you pay for a base plan and get a set number of envelopes per month. For companies with high sales volumes, like telcos, the base plan is quickly exhausted, and extra charges start to add up. In a thriving business, paying per signature is the last place you want to be. The result is a quiet “success tax”: the more journeys you digitize and the more contracts you sign, the more unpredictable your cost base becomes.

From Data Sovereignty to Cost Sovereignty

Today, data sovereignty is forcing many operators away from generic multi tenant SaaS in favour of on premise or sovereign cloud deployments. Once you make that move for compliance reasons, sticking with a per envelope SaaS pricing mentality makes little sense. The same transformation that brings contracts back under your jurisdiction is also an opportunity to bring the cost curve back under your control. In other words, the sovereignty decision forces a deployment change – and that deployment change is exactly what unlocks the opportunity to rethink the pricing model as well.

03 Re-Thinking Digital Contract Deployment Models

It’s time for a new approach – one that solves cost overruns and sovereignty in one step.

Why Sovereignty Bites Harder For Digital Contracts

Once operators accept that generic SaaS is a poor fit for high volume, high risk digital contracts, the next question is not whether to move, but where to move to, and how to pay for it.

Preferred Deployment & Licensing Options

Two combinations stand out for telecoms: on premise with perpetual licensing, and private/ sovereign cloud with term based licensing.

On Premise With Perpetual License

In an on premise model, the digital contract platform runs inside the operator’s own data centres. Infrastructure, access, and change management are handled by internal teams or trusted local partners. This gives the operator a clear, defensible answer when regulators, government customers, or auditors ask where contract evidence resides and who controls it, and it fits naturally alongside other core systems such as billing and CRM.

Perpetual licensing pairs well with this deployment. The operator treats the platform like any other strategic asset: it buys a licence once, deploys on its own infrastructure, and pays a predictable maintenance fee for support and upgrades. Within that environment, usage and storage can be unlimited. This combination is most attractive for stable, high volume workloads and for operators that already favour capex for long lived platforms.

Private/Sovereign Cloud with Flexible Pricing

In a private or sovereign cloud model, the platform runs in a dedicated environment or certified national cloud under in jurisdiction governance. Operators retain the advantages of cloud – elasticity, managed services, and faster provisioning – but with tighter control over data location and legal exposure. In many markets, sovereign clouds are operated in partnership with incumbent telcos, making this a natural extension of their existing role.

This option is commercially flexible, and can be priced with either a perpetual license, term license, or SaaS. Operators can take advantage of unlimited pricing or choose an option that let lets them start small and scale over time. This approach suits those that want the ultimate flexibility, as well as digital only brands, MVNOs, and new market entrants.

A Visual Comparison

Model	Where It Runs	How You Pay	Best Fit
Perpetual On Premise	Operator data centres	Capex + predictable M&S	Core high volume, high compliance workloads
Sovereign / Private Cloud	National or private cloud	Flexible commercials	Digital only brands, MVNOs, pilots, new markets
Generic Global SaaS	Vendor multi tenant cloud	Opex, usage based	Low risk edge cases, if used at all

Trust, Compliance & Long-Term ROI

Building a sovereign digital contract capability – especially on premise or in a private/sovereign cloud – is an investment, but it pays off across three dimensions:

- **Trust & Commercial Differentiation:** Telcos win major deals on trust as much as on price or network quality. This ensures sensitive info never leaves their jurisdiction:
  - Strengthens bids in government and public sector tenders.
  - Reassures large enterprise and wholesale customers.
  - Builds confidence with banks, utilities, and other regulated partners.
- **Compliance & Risk Reduction:** A sovereign platform simplifies compliance and reduces exposure by:
  - Making it clear where contract data resides, which laws apply, and who can access it.
  - Streamlining audits and regulatory information requests.
  - Reducing conflicts between local and foreign legal demands.
  - Allowing consistent retention, deletion, and access policies across all channels.
- **Total Cost of Ownership:** While the upfront cost of a perpetual, sovereign deployment is higher than a small SaaS pilot, over 5–10 years:
  - The effective cost per signed contract falls as volumes grow, instead of rising with every extra envelope or API call.
  - License expansion cycles and SaaS price escalations are avoided.
  - Migration risk is lower: changes in CRM, channels, or cloud strategy don't force a change in the contract platform.

For operators that expect to keep signing millions of contracts every year, the long term case for a sovereign, perpetually licensed foundation is both strategic and economic.

04 Next Steps

Moving Digital Contracts Beyond Generic SaaS

Turning away from generic SaaS for digital contracts is not about rejecting the cloud or abandoning subscriptions. It is about making deliberate choices: deciding where your contracts live, which laws apply to them, who holds the keys, and how their cost behaves as your business grows. For many operators, that will mean anchoring on sovereign deployment models and licensing structures that reward – rather than penalize – higher digital adoption.

The specifics will vary by market, regulatory environment, and investment philosophy. But the direction of travel is clear. Operators who treat digital contracts as strategic infrastructure – and design for both data sovereignty and cost sovereignty from the outset – will be better positioned to win trust, navigate regulation, and scale profitably.

About Maplewave

Maplewave is the premier provider of digital solutions and consulting services for the telecommunications industry. Our goal is to facilitate end-to-end telco transactions in every channel, an approach we call Transact Anywhere. Our solutions connect all channels for a seamless experience - from the warehouse to the customer, and beyond.

Our telecom retail platform unifies all channels – in store, online, indirect, and self service – to create a “transact anywhere” experience. From digital contracts and paperless workflows to inventory, payments, and analytics, we help operators modernize their operations end to end.

With experience across multiple continents and some of the world’s most demanding markets, Maplewave understands the realities of data sovereignty, regulatory complexity, and high volume telecom operations. Our teams combine product, consulting, and implementation expertise to deliver solutions that are both innovative and practical.

For more information about our digital contract solution and how we support sovereign deployments, please **contact us**.

References

Wikipedia. (Data n/a). Data Sovereignty. Retrieved from: **https://en.wikipedia.org/wiki/Data_sovereignty**

WeForm. (2026). Davos 2026: Special address by Mark Carney, Prime Minister of Canada. Retrieved from: **https://www.weforum.org/stories/2026/01/davos-2026-special-address-by-mark-carney-prime-minister-of-canada/**

Wikipedia. (Data n/a). CLOUD Act. Retrieved from: **https://en.wikipedia.org/wiki/CLOUD_Act**

Mimecast. (2025). Why data sovereignty is now a dealbreaker in cybersecurity. Retrieved from: **https://www.mimecast.com/blog/why-data-sovereignty-is-now-a-dealbreaker-in-cybersecurity/**

NovoServe. (2026). Sovereign Cloud Is Just an Illusion: Time for a Strategic Cloud-Exit? Retrieved from: **https://novoserve.com/blog/sovereign-cloud-is-just-an-illusion-time-for-a-strategic-cloud-exit**

Politico. (2026). France to ban officials from US video tools including Zoom, Teams. Retrieved from: **https://www.politico.eu/article/france-ban-officials-us-video-tools-zoom-teams-visio/**

Corporate Compliance Insights. (2018). How the GDPR Will Impact E-Signatures. Retrieved from: **https://www.corporatecomplianceinsights.com/gdpr-will-impact-e-signatures/**

InCountry. (2024). China's digital data sovereignty laws and regulations. Retrieved from: **https://incountry.com/blog/chinas-digital-data-sovereignty-laws-and-regulations**/

SS International. (2025). Cloud Regulation What Legal Teams Must Watch in India's Digital Future. Retrieved from: **https://ssinternational.in/cloud-regulation-what-legal-teams-must-watch-in-indias-digital-future/**

InCountry. (2025). Data residency requirements in LATAM: Brazil, Mexico, and Argentina. Retrieved from: **https://incountry.com/blog/data-residency-requirements-in-latam-brazil-mexico-and-argentina/**

InCountry. (2024). The UK data sovereignty framework: requirements and solutions. Retrieved from: **https://incountry.com/blog/the-uk-data-sovereignty-framework-requirements-and-solutions/**

Macquarie Data Centres. (2024). A Guide to Australian Data Centre Sovereignty. Retrieved from: **https://www.macquariedatacentres.com/blog/a-guide-to-australian-data-centre-sovereignty/**

Impossible Cloud. (2026). Cloud Data Sovereignty for EU Business in 2026. Retrieved from: **https://www.impossiblecloud.com/magazine/cloud-data-sovereignty-for-eu-business-in-2026-new**

Mordor Intelligence. (2026). E-Signature Platform Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031). Retrieved from: **https://www.mordorintelligence.com/industry-reports/global-e-signature-platform-market**

eSignGlobal. (2025). Navigating Canadian Data Residency in E-Signature Solutions. Retrieved from: **https://www.esignglobal.com/blog/canadian-data-residency-e-signature**

Harrison Pensa. (2025). Data sovereignty in Canada: Risks and benefits for businesses. Retrieved from: **https://www.harrisonpensa.com/data-sovereignty-in-canada-risks-and-benefits-for-businesses/**

YourStory. (2025). Data sovereignty and cloud computing: A call to action for Indian businesses. Retrieved from: **https://yourstory.com/2025/02/data-sovereignty-cloud-computing-indian-businesses**

ASPI The Strategist. (2024). Mitigating Australia's cloud-computing risks is still work in progress. Retrieved from: **https://www.aspistrategist.org.au/mitigating-australias-cloud-computing-risks-is-still-work-in-progress/**

Alrafay Consulting. (2024). Comparing On-Premise vs. Enterprise SaaS Solutions: A Comprehensive Analysis. Retrieved from: **https://alrafayglobal.com/on-premise-vs-enterprise-saas-solutions/**

Lemon Learning. (2023). SaaS vs On-Premise software adoption market trends. Retrieved from: **https://lemonlearning.com/blog/saas-vs-on-premise-trends**

EZ Sign. (2025). Signature Market in Canada 2025: Trends, Stats, and Insights. Retrieved from: **https://www.ezsign.com/article/signature-market-in-canada-2025-trends-stats-and-insights/**