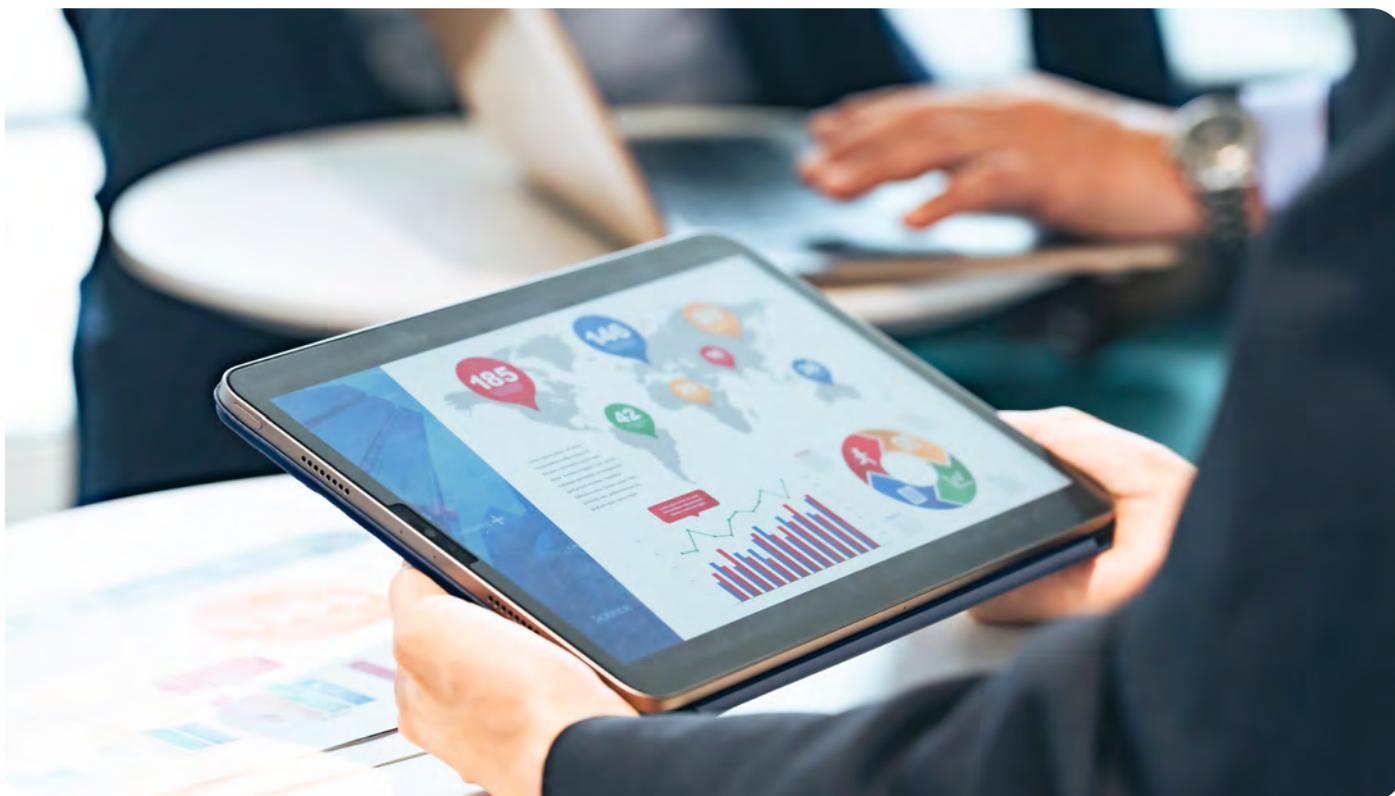# CUSTOMER RELATIONSHIP MANAGEMENT IN A SOVEREIGNTY-DRIVEN WORLD: DISTRIBUTED AND PRIVATE HOSTING

Data sovereignty is reshaping CRM architecture. Organizations are shifting from centralized systems to regional and private deployments. This helps meet regulatory requirements while supporting analytics and global operations.

Ask any global CIO about today's most material digital risks, and data sovereignty is likely to feature prominently. Governments are asserting stronger control over where data must reside, how it is processed, and who can access it. There is no single global set of data rules. Instead, countries enforce their own laws at the same time.

> For example, the EU's General Data Protection Regulation and China's Personal Information Protection Law look similar in structure, but they require different things in practice such as where data must be stored, what permissions are needed to use it, and how violations are punished.

For multinational companies, this means they must follow multiple country-specific rules at once, along with new cloud, AI, and data protection laws emerging across the Middle East, India, Australia, and Latin America.

In this environment, enterprises are no longer free to centralize sensitive customer information in one global cloud. Instead, they are increasingly required to ensure that personal, financial, healthcare, citizen, or operational data never leaves national borders. This pressure is already being felt: 92% of business leaders are actively revisiting their cloud strategies to include hybrid, in-country, sovereign, or private-hosted options.

For customer relationship management (CRM) systems, the stakes are even higher. Platforms like Salesforce, SAP, and Microsoft Dynamics were built around the idea of one global source of truth. Centralized architecture meant simpler governance, unified workflows, and a consistent reporting backbone. Today, however, regulatory expectations are pushing enterprises to re-evaluate that model and to adopt region-aware deployment patterns, but without losing the cohesion and efficiency of a global CRM strategy. Balancing those two forces is where the complexity begins.

Sovereignty pressures

As organizations adapt to sovereignty expectations, CRM platforms frequently encounter practical challenges. The nature of challenges is driven by the combination of regulated data types managed in CRM and the global nature of the processes it supports. Three issues tend to surface most often:

1. Aligning centralized CRM designs with data-handling requirements: CRM platforms work best when customer records, workflows, and analytics operate from a unified environment. But when certain categories of data must remain within national borders, managing data location becomes necessary for regulatory compliance. In those cases, organizations sometimes need to introduce

regional processing or regional data stores. This doesn't mean building entirely separate CRMs, but it does require architectural adjustments that increase design, governance, and operational complexity.

2. Handling cross-border data movement limitations: Global integrations and operations often depend on data moving freely across regions, particularly systems that rely on data analytics and business intelligence. However, with regulations preventing certain data types from leaving a jurisdiction, the existing workflows, integrations, or processing steps must be redesigned so they can run locally and continue existing operations. These localized modifications add effort, introduce additional testing paths, and require more careful life cycle management.

3. Cost and operational overhead for distributed architectures: A single global CRM environment is generally simpler and more economical to run. When parts of the CRM landscape need to be distributed or when local processing paths are introduced, the organization has more environments to coordinate, more integrations to maintain, and more monitoring and testing to perform. These costs are not mandated by law but arise from the architectural decisions enterprises make to meet sovereignty

requirements while keeping global CRM functionality intact.

The shift to sovereignty-ready CRM

As data-sovereignty pressures increase, CRM platforms are evolving from centralized designs to architectures that can operate flexibly within local regulatory boundaries. Rather than sending all customer interactions, workflows, and analytics through a single global system, many organizations are now adopting CRM strategies that allow sensitive data to remain within national borders while still supporting a coherent, enterprise-wide experience. This approach helps meet growing residency and privacy expectations without undermining the consistency, governance, or shared processes that large organizations rely on.

In practical terms, this shift involves moving CRM components such as customer data records, interaction histories, business rules, integrations, and reporting tools from isolated systems to multiple cloud regions or, where necessary, to local customer-controlled facilities. The intention here is to build a federated environment in which each region can handle regulated data locally, while the broader CRM landscape remains aligned through shared metadata, common configuration patterns, and centrally

managed governance structures. This means complying with local regulatory requirements while avoiding rearranging everything in an existing architecture.

One illustration of this approach comes from a large American bank holding company that collaborated with Infosys to modernize its multiorganization Salesforce architecture to better support regulatory and operational priorities. With more than 40 production and non-production environments across multiple business lines, the company needed clearer control over where customer and financial data was processed, while maintaining stability and scale to comply with regulatory requirements. With the help of Infosys, the bank reorganized its CRM architecture to operate in a more region-aware and modular manner. Through coordinated analysis, regression testing, and phased upgrades, it deployed Salesforce in a way that it can work differently across regions, rather than being forced into a standard, centrally hosted setup. As a result, regulatory alignment improved because customer and financial data could be processed and stored closer to where regulations require it. At the same time, scalability improved because different regions or business units could scale their Salesforce environments independently. The organization gained more control over where Salesforce runs and how it is structured, while still using the Salesforce platform.

A Swiss multinational pharmaceutical company similarly needed to comply with EU and Swiss data residency requirements while maintaining security and performance across a large Salesforce footprint. With more than 70 production Salesforce organizations operating across Europe, the existing setup made it difficult to ensure that regulated patient and operational data remained within approved jurisdictions. The company selected Salesforce Hyperforce to manage its data landscape by deploying Salesforce applications and services in approved regional cloud locations. The resulting CRM environment handled regulated data locally while supporting improved security and performance without disrupting business operations.

A foundation for regional CRM hosting

These examples are part of a wider trend across regulated industries. Many organizations are now using regional cloud hosting as part of their CRM modernization to meet data residency, security, and performance requirements.

For the American bank holding company, Hyperforce strengthened CRM modernization by improving data residency governance and alignment with US regulatory

expectations. For the Swiss multinational pharmaceutical company, the use of Hyperforce supported compliance with EU and Swiss data residency rules while maintaining secure and reliable CRM operations.

A similar approach was used by several telecommunications providers in Australia and New Zealand, which were required

> Platforms like Salesforce Hyperforce allow companies to run their CRM systems in approved locations while keeping the core Salesforce features intact. This makes it easier to design CRM setups that respect regional rules without breaking existing operations.

to keep sensitive personal data, such as customer names and contact details, within their respective countries to meet data residency requirements. In their earlier setup, Salesforce was hosted outside the ANZ region, while sensitive data was stored in external databases hosted locally within Australia or New Zealand. Salesforce accessed this data through integrations to comply with residency rules.

By adopting Salesforce Hyperforce, these providers were able to deploy Salesforce directly in approved in-country cloud regions. With Hyperforce running on local AWS infrastructure, Salesforce itself could store and process sensitive data within national borders. This allowed the external databases to be retired, simplified integrations, and consolidated security, governance, and access controls within Salesforce.

From regional cloud CRM to on-premises

While Hyperforce helps organizations meet data residency requirements by placing data in local cloud regions, it does not fully address the needs of the most tightly regulated industries. In these sectors, regulators also care about who controls the infrastructure, who has administrative access, and how systems are operated and monitored. Simply running CRM in a local public cloud region is not always enough.

As these expectations expand beyond data location to include infrastructure control and operational assurance, private hosting is becoming more relevant. This provides stronger control over infrastructure while still retaining the automation, scalability, and security features associated with cloud platforms. Private hosting is particularly useful for scenarios that require very low latency or strict locality, such as trading environments, manufacturing systems, hospitals, or national service centers. By keeping CRM systems close to

critical enterprise platforms and data sources, organizations can meet regulatory and resilience requirements without limiting modern CRM capabilities.

> Private hosting allows organizations to run Salesforce using hyperscaler technologies such as AWS Outposts, Azure Stack, Google Anthos, or Alibaba Apsara Stack within their own facilities or approved co-location sites.

What to expect with private CRM hosting

Running Salesforce on hyperscaler-managed private infrastructure gives organizations more control over where data is stored and how infrastructure is managed, but it also changes how Salesforce operates day to day. Decision-makers need to evaluate the extra responsibilities that come with private hosting.

1. Decision on the upgrade cycle: When Salesforce runs on customer-specific private infrastructure managed by a hyperscaler, upgrades and maintenance no longer happen automatically on a fixed schedule. Salesforce continues to manage the core platform, but the organization must coordinate with Salesforce, the hyperscaler, and the system integrator to plan maintenance windows, upgrades, testing, and release timing. This means upgrades need to fit around business operations rather than happening entirely in the background.

2. Change in the level of control: With private hosting, organizations gain control over infrastructure, networking, and security settings such as firewalls, access rules, and encryption. However, Salesforce platform limits still apply. Usage limits remain in place, and some platform services continue to be shared and managed by Salesforce. This means greater control over infrastructure, but not full control over how the Salesforce platform operates, so responsibilities must be clearly defined.

3. Customized disaster recovery: Unlike public cloud or regional deployments where recovery is more standardized, private hosting requires customized disaster recovery planning. This includes defining how data is replicated, how backups are taken, and how failover is tested. These plans are designed and validated jointly by Salesforce and the organization and require more involvement from internal teams.

4. Multicountry operations add more complexity: For companies operating across multiple countries or running many Salesforce organizations, private hosting can help by keeping data in specific locations and improving performance for local users. At the same time, managing multiple environments adds complexity. Decisions need to be made about how many Salesforce instances to run, how they connect to each other, and how consistency is maintained across regions.

5. Physical readiness matters: Private hosting requires space in a data center or colocation facility, reliable power and cooling, robust network connectivity, and physical security. Capacity is more limited than in the public cloud, and installation, shipping, and integration with existing systems must be planned carefully.

6. Extra caution while testing: Finally, while Salesforce and hyperscaler providers test platform upgrades and provide monitoring tools, customer testing and validation remain essential. Private hosting works best for organizations with strong regulatory drivers, mature cloud operations, and clear data residency requirements. It offers greater control and compliance, but it also requires careful planning and acceptance of added operational complexity.

What enterprises should do next

Organizations should start by clearly identifying what customer and operational data they hold and which data is subject to residency or transfer restrictions. This helps determine what parts of the CRM system must stay local and what can operate globally, and how much distribution or private hosting is actually required.

The next step is to design CRM environments that meet regional requirements without creating fragmentation. Even when data cannot move across borders, regional Salesforce organizations should follow common configurations, workflows, and governance standards. The goal is a federated CRM setup where regional systems are aligned rather than isolated.

Choosing the right hosting model is also important. Regional cloud deployments may be sufficient for many organizations, while those with stricter security or residency requirements may need private hosting on hyperscaler-managed on-premises platforms. This requires checking facility readiness, such as power, cooling, and network connectivity, and understanding how responsibilities are shared between Salesforce, the cloud provider, and the system integrator.

Finally, organizations should ensure that regional CRM environments can run independently when needed, while still sharing non-sensitive data where permitted. This supports global reporting and analytics without violating data regulations and allows advanced capabilities, such as AI, to be used responsibly by keeping sensitive data local.

The new CRM frontier

As regulations change across countries, data sovereignty is becoming one of the priority issues in boardroom discussions. It directly affects how CRM systems are designed and run, especially because leaders need to decide on where customer data is stored, how it is processed, and how data moves across regions. To address this, organizations are increasingly using regional cloud deployments, federated CRM setups, and, where required, private hosting to keep regulated data within national borders. By aligning CRM architecture with these requirements, enterprises can continue to use analytics and AI within regulatory limits, support local operations, and maintain CRM environments that are compliant, resilient, and sustainable over the long term.

Authors

Sam Boban | Mysuru
Kiran Chandragouda Patil | Canada
Dr. Thejasvi Nagaraju | Mysuru
Taniya Chandra | Bengaluru

Editorial and production

Kate Bevan | London
Pragya Rai | Bengaluru

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.

To view our research, visit Infosys Knowledge Institute at infosys.com/IKI or email us at iki@infosys.com.

For more information, contact askus@infosys.com

Infosys.com | NYSE: INFY

Stay Connected