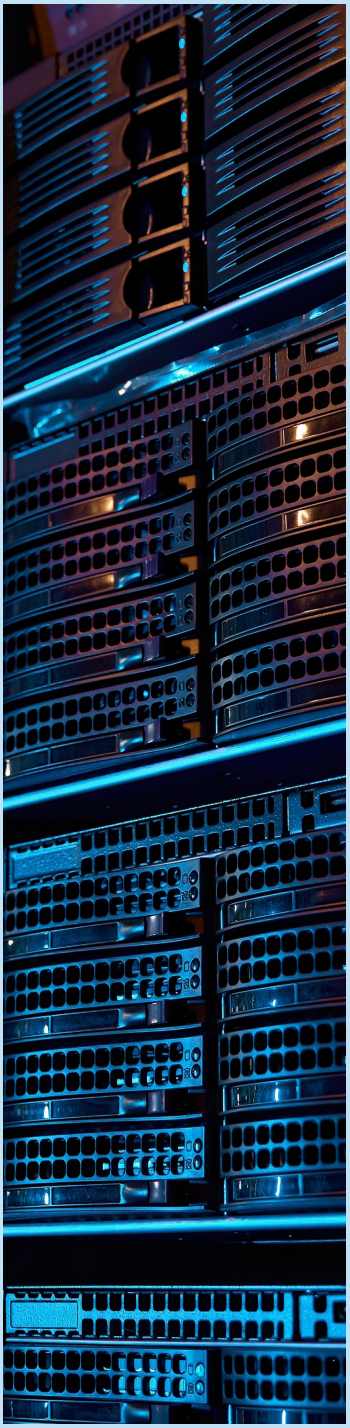
VIEW POINT



NAVIGATING DATA RESIDENCY FOR FINANCIAL SERVICES: ESSENTIAL COMPLIANCE STRATEGIES

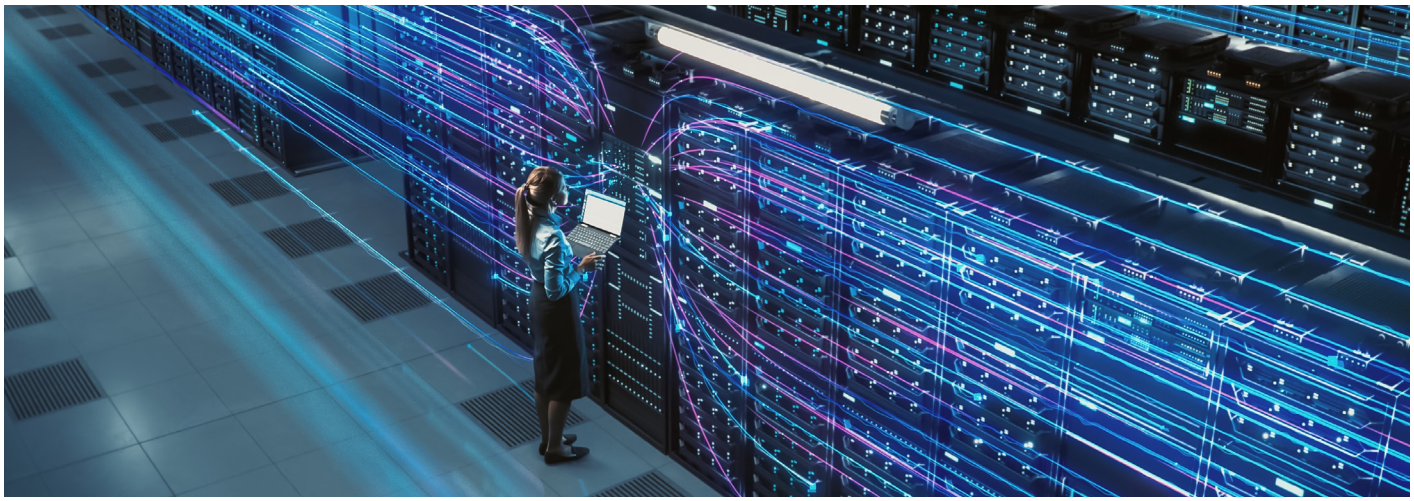
Abstract

Financial institutions handle vast volumes of sensitive customer and transactional data. With the growth of digital banking, cloud adoption, and global operations, the risks of storing and processing data beyond national borders have intensified. These institutions continually face the challenge of balancing digital innovation with stringent regulatory compliance. At the core of this challenge lies data residency. As regulations tighten worldwide and jurisdictions assert control over digital data, financial institutions must respond quickly.

This article examines how financial services firms can strategically navigate data residency requirements, maintain compliance, and strengthen financial services data protection in an evolving regulatory landscape

Infosys®
Navigate your next

What is data residency, and why does it matter



Data residency refers to the requirement that data be stored in a specific country or region. It ensures compliance with local laws, supports national security, and protects privacy. Over 135 countries have introduced data localisation laws, with around 75% enforcing rules that impact financial institutions. These mandates require banks and financial service providers to store and process data within national borders, maintain strong oversight, and ensure lawful access. For the financial sector, data residency is a pillar of operational resilience, customer trust, and regulatory alignment.

Data residency compliance challenges

While the concept of data residency may appear straightforward, putting it into practice across globally distributed operations is anything but. Data residency introduces a complex set of operational, legal, and technological hurdles. Below are some key challenges financial firms must address:

Cloud computing and data location ambiguity

Public cloud environments can shift data across borders, making it difficult for financial institutions to ensure sensitive data stays within legally approved jurisdictions, increasing compliance and regulatory risk.

Navigating multi-jurisdictional compliance requirements

Financial institutions operating across borders face the risk of falling short of overlapping data residency laws such as the GDPR. Without aligning data policies to the most stringent local requirements, they risk legal exposure, operational disruption, and restricted data flows.

Clarifying data residency vs. Data sovereignty

Compliance programs must differentiate between the physical location of data and the legal authority governing it. Hosting data locally does not guarantee compliance if foreign vendors manage it under different access, audit, or disclosure regulations.

Balancing compliance with operational efficiency

Strict data residency laws can lead to fragmented infrastructure and increased IT complexity. Institutions must meet compliance requirements without compromising agility, resilience, or critical functions like risk modelling, fraud detection, and regulatory reporting.

Managing vendor and third-party compliance risks

Reliance on third-party vendors can expose financial institutions to data residency violations if those partners lack proper controls or operate outside approved jurisdictions. Institutions remain accountable and must enforce compliance through due diligence, strong contracts, and continuous oversight.

Adapting to evolving regulatory landscapes

Financial data residency rules are rapidly changing due to privacy concerns and geopolitical shifts. Institutions risk non-compliance unless they implement flexible cloud and governance frameworks that can quickly adjust to new laws, especially in sensitive or fast-growing markets.

Navigating the path forward: key strategies for compliance

Despite data residency challenges, financial institutions can ensure compliance without sacrificing agility by integrating IT, legal, and vendor management. Adopting best practices transforms compliance from a burden into a strategic advantage.

Adopt hybrid cloud architectures

By 2027, 90% of enterprises will implement hybrid cloud models. A hybrid cloud approach allows organisations to store sensitive or regulated data locally while using public cloud infrastructure for other workloads.

For example, many multinational enterprises use private clouds or on-premises solutions in countries with strict data residency laws, while deploying public cloud resources for less sensitive operations. This model ensures compliance without sacrificing scalability or performance.

Implement advanced encryption

Encryption plays a critical role in protecting data, especially when compliance requires it to remain within specific jurisdictions. Encrypting data at rest and in transit, along with techniques like tokenisation and encryption in use, helps organisations maintain control even in distributed environments.

For instance, companies processing personal data under regulations like GDPR often use strong encryption protocols to prevent unauthorised access, even when leveraging regional cloud infrastructure.

Use local data centres

One of the most direct methods to meet data residency requirements is selecting cloud or colocation providers with data centres in the required geography. Major hyperscale cloud providers continue to expand their local infrastructure into more regions.

This helps businesses store regulated data within required borders while still benefiting from the advantages of cloud computing.

Deploy Cloud Access Security Brokers (CASBs)

CASBs provide organisations visibility and control over cloud data usage. These tools can enforce location-based policies to ensure data does not leave specific jurisdictions.

For example, companies operating in multiple countries can use CASBs to monitor cloud usage and restrict cross-border data flows, ensuring regional compliance without disrupting workflows.

Enable geofencing and granular access controls

Geofencing restricts data access based on geographic location, helping prevent unauthorised cross-border access. Combined with Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA), it ensures only authorised users within compliant regions can view or process sensitive data.

Organisations in regulated industries such as finance and healthcare often rely on these controls to align with national data requirements and reduce compliance risks.

Train staff on data residency requirements

Compliance requires staff awareness. Employees should be trained to recognise what types of data are subject to residency requirements and how to handle them appropriately.

This includes understanding risks like uploading files to unauthorised platforms, forwarding sensitive emails, or using cloud apps that store data outside approved regions. Regular training helps avoid accidental violations and promotes a culture of compliance.

Maintain ongoing engagement with legal and compliance teams

Data residency rules can vary across regions and evolve. Collaborating with internal legal and compliance experts ensures your organisation stays aligned with the latest regulatory expectations. This is especially important for companies operating across borders, where overlapping or conflicting rules may apply. Routine audits, policy updates, and risk assessments are essential to ensure your data infrastructure remains compliant as your business grows.

The high stakes of falling short

While adopting best practices can significantly reduce the risk of non-compliance, failing to meet data residency obligations carries serious consequences. For financial institutions operating in a highly regulated and trust-sensitive environment, the cost of getting it wrong can be steep, impacting operations, legal standing, market access, and brand reputation. Here's what's at stake when compliance is overlooked.

Legal sanctions and business restrictions

Non-compliance may result in hefty fines, sanctions, or restrictions on operating within certain jurisdictions. Many countries enforce strict data storage and processing rules, especially for personal and financial data.

Operational disruption

Sudden mandates to localise or migrate data can force institutions into unplanned infrastructure changes, disrupting services, increasing costs, and diverting resources from innovation.

Limited market and contract access

Firms that fail to meet local residency standards may be barred from entering regulated markets or bidding for public sector contracts, limiting growth opportunities.

Regulatory scrutiny and oversight fatigue

Violations often lead to increased audits, reporting burdens, and prolonged engagements with data protection authorities, straining compliance teams and exposing more areas to risk.

Reputational damage and loss of trust

Customers and partners expect transparency and legal alignment. Any lapse in compliance, especially involving data, can erode confidence, attract media attention, and trigger customer attrition.

Increased cybersecurity exposure

Hosting data in unregulated or non-compliant jurisdictions can weaken protections and increase exposure to data breaches, surveillance, or access by foreign entities, compounding legal and security risks.

Case in point: Following previous GDPR violations, a multinational financial services firm now enforces robust data residency controls across its EU operations. It leverages local cloud infrastructure, implements encryption for data at rest and in transit, and enforces role-based access controls, ensuring regulatory compliance and restoring customer confidence.

Emerging trends in data residency compliance

As global regulations evolve, several key trends are reshaping how financial institutions manage data residency. One of the most impactful is the rise of Regulatory Technology (RegTech). These tools help automate compliance monitoring, enforce cross-border data policies, and offer real-time visibility into data flows. Financial institutions are increasingly integrating RegTech solutions with cloud governance frameworks to reduce manual oversight, improve accuracy, and respond faster to shifting regulatory landscapes. By the end of 2025, over 60% of compliance leaders plan to invest in AI-powered RegTech to enable more proactive, scalable oversight.

We're also seeing deeper collaboration between regulators and cloud providers to build location-specific compliance frameworks, allowing innovation to thrive without compromising legal obligations. These tech-enabled strategies are essential for financial institutions aiming to future-proof their compliance posture.

From obligation to opportunity: rethinking data residency

Data residency should be seen as more than just a compliance requirement to avoid fines or penalties. It's more than just where data lives. It's about how responsibly institutions handle it. In a market defined by trust and accountability, that distinction makes all the difference.

Forward-thinking financial institutions treat compliance as an integrated part of digital transformation. These institutions embed regulatory awareness into cloud strategy, security practices, and vendor management.

More than a regulatory exercise, sustainable data residency compliance requires embedding the right mindset across the organisation. It requires fostering a culture where compliance becomes second nature and is supported by leadership, collaboration, and transparency.

By doing so, financial institutions unlock operational agility, sustain growth, and build stronger customer relationships that reinforce digital trust.

Your next step in data residency readiness

To future-proof your institution, combine legal vigilance with technical innovation. Create adaptable architectures, invest in compliant cloud solutions, and embed financial services data protection into your organisational DNA. Data residency compliance can then evolve into a business advantage that fuels safer growth.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next