

Data Residency in a CDP: Why Location of Data Matters for Regulated Industries



For regulated organizations such as banking, financial services, healthcare, insurance, and telecommunications, data residency in a CDP is not a technical detail, it's a compliance obligation. Where customer data is stored determines which laws apply, who can access it, and what happens when regulations change. This paper outlines why it matters, what's at stake, and what to look for in a compliant CDP.

What Is Data Residency and Why Does It Matter?

Data residency refers to the geographic location where data is stored and processed. For regulated industries, this has direct legal consequences. Many jurisdictions now require that customer data — particularly financial, health, and identity data, remain within national borders.

The Risks Of Getting It Wrong Are Significant:



**REGULATORY FINES
AND LICENCE
SUSPENSIONS**



**FAILED AUDITS AND
LOSS OF
COMPLIANCE
CERTIFICATIONS**



**EXPANDED BREACH
EXPOSURE ACROSS
UNCONTROLLED
INFRASTRUCTURE**



**REPUTATIONAL
DAMAGE THAT IS
DIFFICULT TO
RECOVER FROM**

The Regulatory Landscape

Regulation	Region	Requirement
GDPR	European Union	Data must stay within EU/EEA or approved jurisdictions
RBI Guidelines	India	Financial and payment data must be stored on Indian soil
PDPA	Thailand	Restrictions on cross-border transfer of sensitive data
PDPL	Saudi Arabia	Personal data processing limited within Kingdom boundaries
PIPL	China	Strict localisation for personal information processing

What a Compliant CDP Must Deliver



01. In-country deployment options

on-premises, private cloud, or sovereign cloud regions



02. Single-tenant infrastructure

no commingling of customer data across organisations



03. Data flow auditability

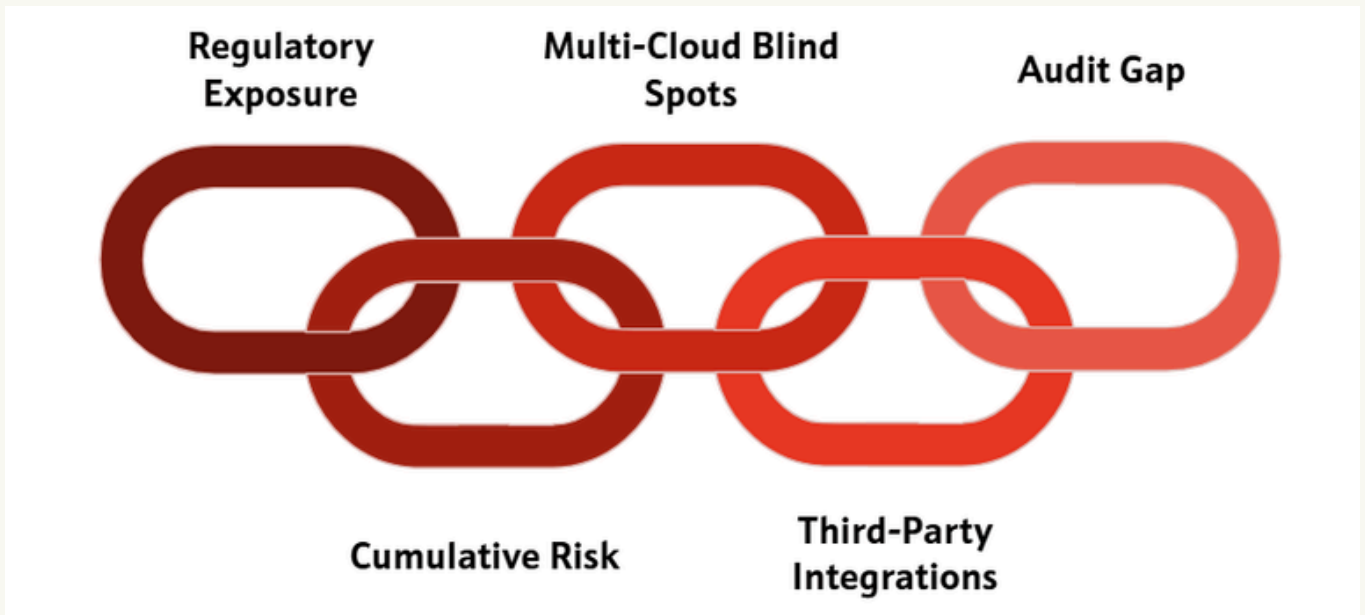
clear, documented evidence of where data lives and who accesses it



04. Granular access controls

preventing cross-border data access by role or geography

The Hidden Risks of Non-Compliant CDP Deployments



Key Questions to Ask Your CDP Vendor



Data Locations:

Can you specify data centre locations and cloud regions?



Isolation & Tenancy:

Is our environment fully isolated?



Lineage & Audits:

Can you provide data lineage on demand?



Integration Controls:

How are third-party integrations controlled?

Not sure what to ask your CDP vendor? Dive deeper with [6 QUESTIONS TO ASK ANY CDP VENDOR BEFORE SIGNING](#), our step-by-step guide to evaluating platforms before you commit

Conclusion

Data residency has moved from a back-office issue to a boardroom priority as global regulations tighten. **Lemnisk's** Composable CDP is built for regulated industries, offering in-country deployment, single-tenant infrastructure, and audit-ready governance—without sacrificing real-time personalization.

[Get a Demo Now](#)

