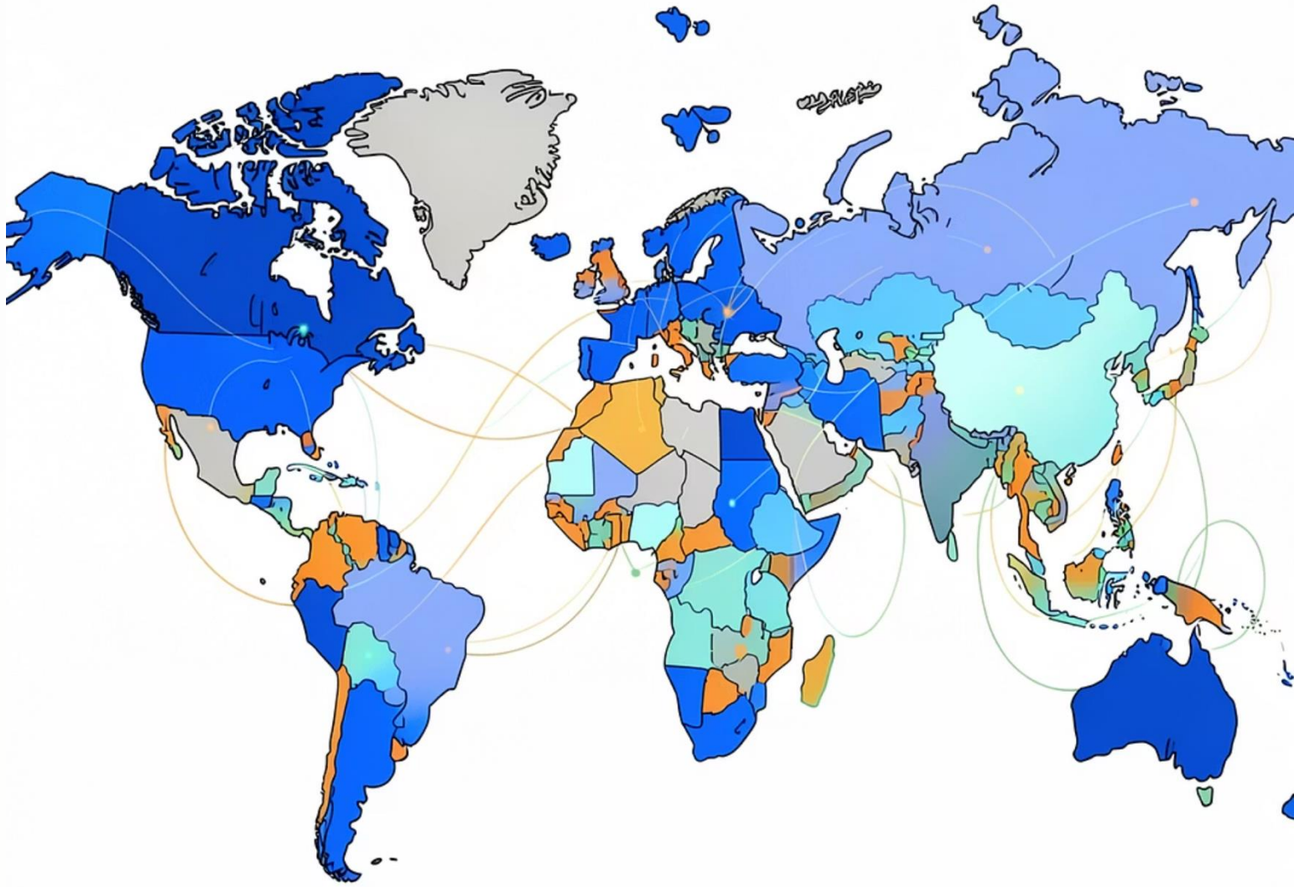
The Effects of Deglobalization on Enterprise Technology

A Capstone Presentation for JPMorgan Chase

Geopolitical tensions will likely intensify rather than stabilize, prompting further technology restrictions, data localization mandates, and vendor exclusions.

JPMC's ability to remain operational across the EU, India, and China depends not on finding a unified solution, but on building a legally sound, technically cost-effective, and compliant policy across three incompatible regimes simultaneously.



OUR TEAM TODAY

Meet the Team

Kankon Sen

Nicole Wang

Ethan Sheinker

Wei Gan

Sofia Marrero

Kylee Zhou

Arnav Sahai

OUR AGENDA TODAY

Agenda

A structured briefing on digital sovereignty and its operational implications for JPMorgan Chase.

Chapter 0

Macro Context

- Sovereignty
- Impact of Sovereignty Regimes on Tech Stacks
- Why Sovereignty Now?
- Where Sovereignty Is Emerging

Chapter 1

European Union

- The EU Sovereignty Framework
- EU: Macro Drivers & Direct Impacts

Chapter 2

India

- India: Compliance as a Strategic Advantage
- India: Macro Drivers & JPMC Implications

Chapter 3

China

- China: Regulatory Framework
- China: Direct & Indirect Impacts on JPMC

Strategic Analysis

Cross-Jurisdictional Matrix

- Thematic Risk Matrix

Conclusion

Recommendation

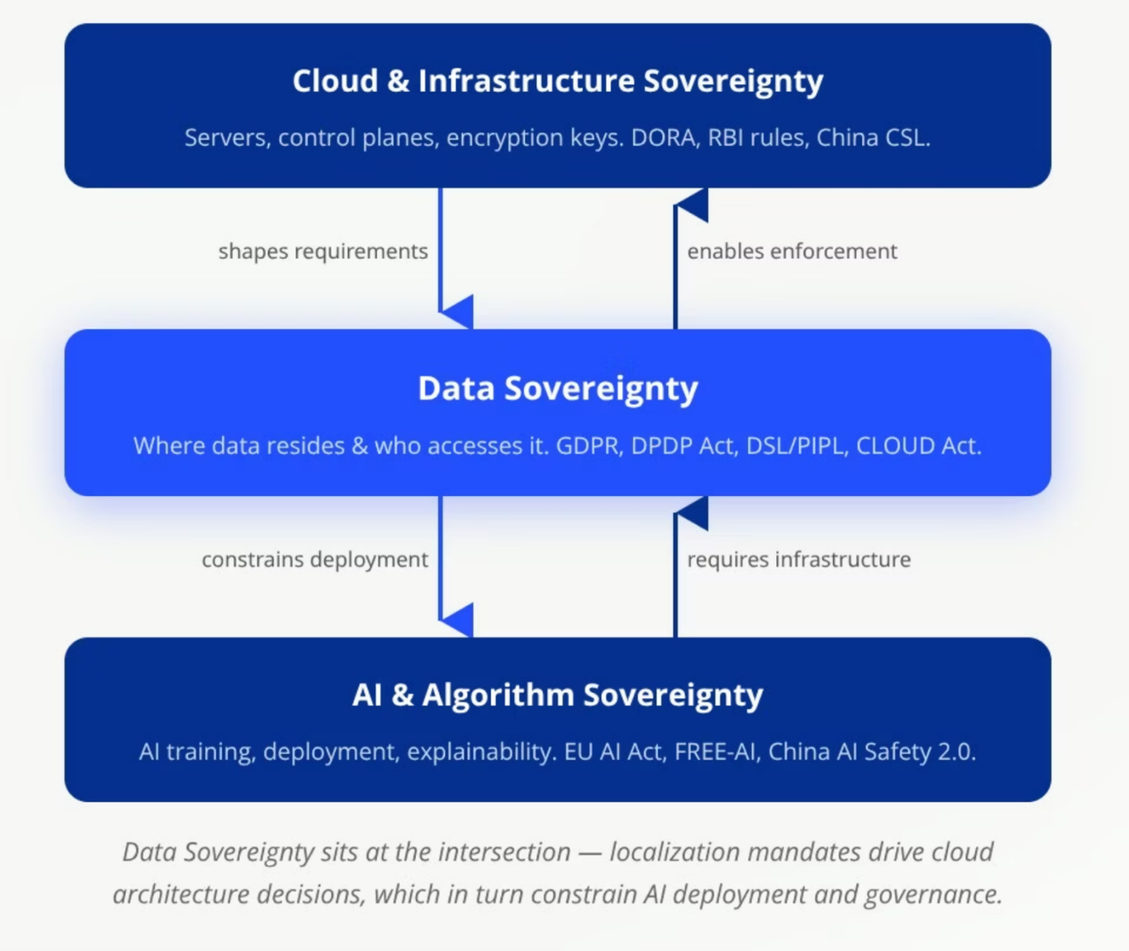
- Pros & Cons

MACRO CONTEXT

Sovereignty

Technology Sovereignty

The overarching political objective — national capacity to independently develop, control, and fund core digital technologies. Key laws: EU CADA (Q1 2026), China 15th FYP, India AI Mission.



Data Sovereignty sits at the intersection — localization mandates drive cloud architecture decisions, which in turn constrain AI deployment and governance.

MACRO CONTEXT

Sovereignty vs. Related Concepts

Sovereignty is the overarching political narrative — but it is frequently conflated with adjacent concepts. Understanding the distinctions is essential for precise regulatory analysis.

Sovereignty

The umbrella political narrative. Jurisdictional authority, vendor independence, and self-determination — the framework under which all other concepts are justified.

Resilience

Ability to withstand and recover from disruptions. Sovereignty rhetoric directly drives resilience mandates such as CRA.

Privacy

Protection of individual rights over personal data. Privacy was the first wave of sovereignty-adjacent regulation — GDPR is the clearest example.

Security

Protection from threats and vulnerabilities. Cybersecurity is a technical prerequisite for sovereignty, not a substitute for it.

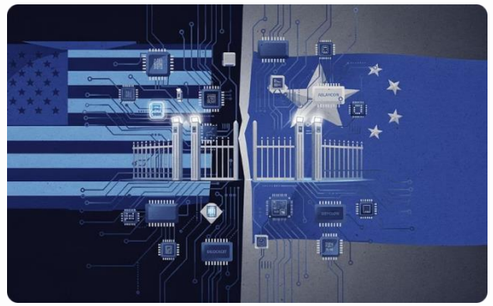
Data Localization

Physical residency of data within borders. The most concrete, enforceable manifestation of data sovereignty — but not the whole picture.

CONTEXT

Sovereignty Is Rewriting the Tech Stack

Three structural forces are converging to make digital sovereignty the defining regulatory challenge for global financial institutions.



Geopolitical Fragmentation

US–China strategic competition is splitting technology ecosystems and pushing states to align digital rules, vendors, and infrastructure with national-security priorities rather than global efficiency

Domestic Politics

Domestic regulators and security agencies frame foreign tech dependence as a liability for jobs, privacy, and critical infrastructure — lawmakers hard-code sovereignty through localization mandates, sovereign clouds, and stronger state audit powers over data and vendors

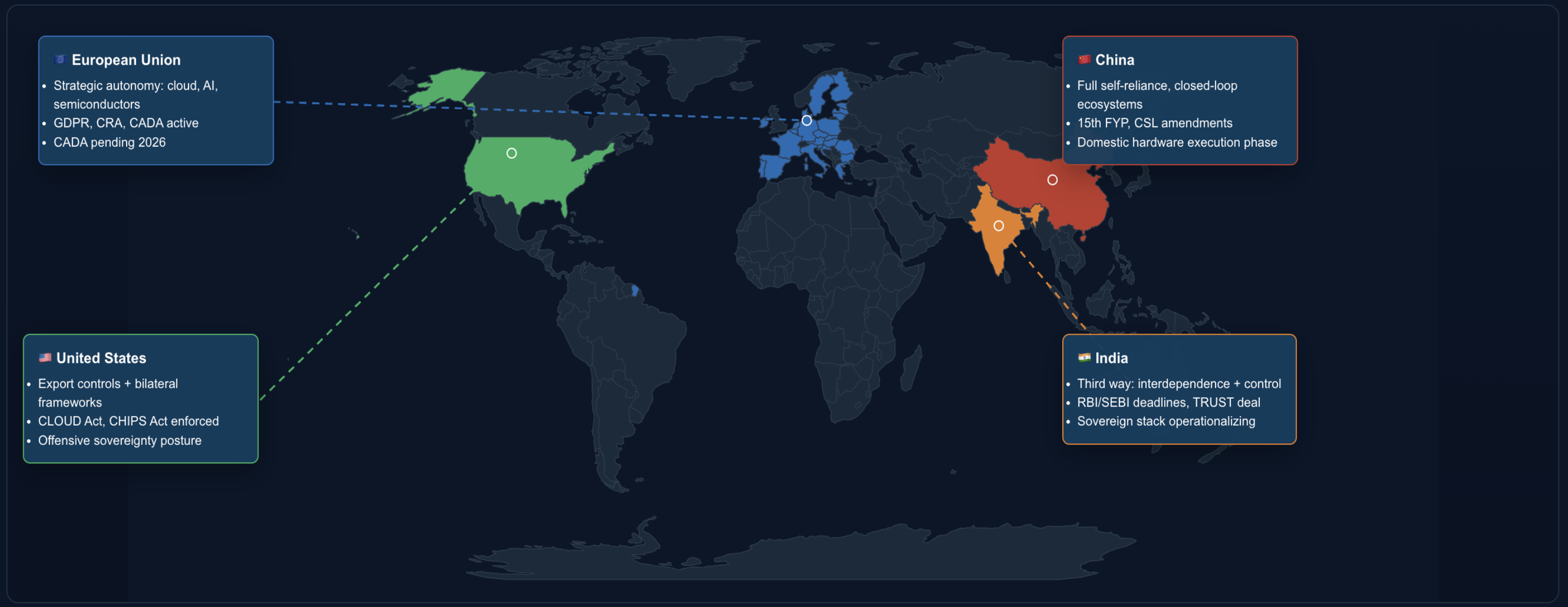
Control Over Data and Infrastructure

States increasingly treat data, cloud, AI, and technology infrastructure as strategic assets — driving localization, domestic vendor preferences, and stricter sovereignty regulations that challenge globally integrated operations

MACRO CONTEXT

Where Sovereignty Is Emerging

Sovereignty mandates are no longer confined to the EU — they represent a global structural shift across every major economic bloc.



65%
Governments introducing sovereignty requirements by 2028

$100B+
Global sovereign AI compute commitments in 2026

2×
Expected growth in non-U.S./China AI compute share by 2030

The EU Sovereignty Framework

CHAPTER 1 — EUROPEAN UNION

EU Cyber Resilience Act (CRA)

In force as of December 2024 and fully applicable by December 2027

Mandates cybersecurity for all "Products with Digital Elements"

General Data Protection Regulation (GDPR)

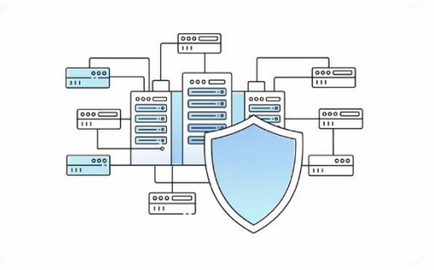
Published in 2016 and fully applied in 2018

Designed to protect individuals' rights to privacy and data protection within the EU

EU Cloud and AI Development Act (CADA)

scheduled for proposal in the first quarter of 2026

Represents the EU's industrial policy objective



European Cloud Services Scheme (EUCS)

drafted in December 2020

Creates unified cybersecurity certification standards for cloud services across the EU

Different Opinions: France and Germany

Sources: European Commission. "Cyber Resilience Act." Shaping Europe's Digital Future. Intersoft Consulting. "General Data Protection Regulation (GDPR)." European Commission. "Cloud and AI Development Act." European Union Agency for Cybersecurity (ENISA). "EUCS – Cloud Service Candidate Cybersecurity Certification Scheme." August 2023.

CHAPTER 1 — EUROPEAN UNION

EU: Macro Drivers & Implications

Macro Drivers

Pursuit of Strategic Autonomy

To establish an independent technological framework and reduce overreliance on non-EU tech giants.

Correcting Market Failure

The EU aims to correct market failures caused by information asymmetry and negative externalities.

Addressing the Legal Deadlock

Resolving the conflict between the extraterritorial mandates of the U.S. CLOUD Act and the EU's GDPR.

Implications on Banks

Legal Deadlock

Compliance with one jurisdiction requires violating the other — up to 4% of annual revenue at risk.

Vendor Lock-In

Compliance costs may drive smaller, innovative vendors out of the market, reducing competitive choice.

Rigorous Cloud Review

Cloud providers must undergo rigorous independent certification under EUCS High Assurance standards.

Higher Costs

Higher taxes and inflated service prices as compliance overhead is passed through the supply chain.

The EU's digital sovereignty is gradually being translated into binding operational standards, ensuring that its core digital assets remain independent and controllable through the integration of legal shielding, sovereign cloud, and localized computing.

India: Local Control, Global Access

CHAPTER 2 — INDIA

RBI April 10 Deadline

Firms must give the RBI unfettered audit access to cloud and IT outsourcing. Local control remains mandatory.

DPDP Act & Data Protection Board

JPMC is a Significant Data Fiduciary, requiring more audits and stronger local data governance.

Local Key Control

BYOK and local key control keep Indian data under Indian jurisdiction across global operations.

SEBI Cybersecurity Framework

Systemically important firms must appoint a Resident Designated Director with personal legal accountability.

Sources: RBI Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102, April 10, 2023) — sets the three-year compliance runway ending April 10, 2026. The DPDP Act 2023 & DPDP Rules 2025 create a horizontal compliance regime for all financial data fiduciaries (King, Stubb & Kasiva, January 2026). The SEBI CSCRF framework mandates a Resident Designated Director with personal statutory accountability.

CHAPTER 2 — INDIA

India: Macro Drivers & JPMC Implications

Macro Drivers – Strategic Interdependence

India treats digital infrastructure as a tool for local control, economic strategy, and national security.

Pax Silica Declaration (Feb 2026)

India agreed to easier access to advanced U.S. hardware in exchange for local data control and trusted-node status.

2047 Tax Holiday

India is using tax incentives to encourage local sovereign cloud and AI infrastructure development.

Sovereign AI Models

Local data must stay in India, and model development is expected to remain under Indian oversight.

FREE-AI Committee

AI credit and risk models may face explainability and audit requirements.

Direct Implications for JPMC

Contractual Enforcement (April 10)

Mandatory inclusion of 'unfettered audit access' and 'right to inspection' clauses in all IT and cloud contracts.

Localized Governance & Liability

Appointment of a Resident Designated Director and India-based Data Protection Officer with personal legal accountability and 2-hour 'technical glitch' reporting.

Accelerated Incident Response

Transition from the global 72-hour reporting window to the mandatory 6-hour CERT-In window for cyber incidents.

Sovereign Key Management

BYOK encryption hosted on Indian soil insulates Indian client data from U.S. CLOUD Act warrants served at the global level.

Looking Ahead: Local AI Oversight

By late 2026, India may require more explainability and auditability for AI-driven credit and risk models, raising the bar for how those systems are deployed and governed.

Looking Ahead: Local Cloud Standards

As India expands its cloud and data rules, firms may face more requirements around reporting and managing the footprint of local data workloads.

CHAPTER 3 — CHINA

China's Regulatory Framework

Cybersecurity Law (CSL)

Governs critical information infrastructure operators; mandates domestic data storage and security reviews.

Data Security Law (DSL)

Classifies data by national importance; restricts cross-border transfers; Art. 36 blocks foreign legal demands.

Personal Information Protection Law (PIPL)

China's comprehensive personal data law; governs consent, processing, and cross-border transfer of personal information.

Data Localization & Transfer

- FIs classified as CIIOs must store data on domestic servers
- Core and important data cannot leave China without government approval
- Outbound transfers require CAC security assessment at large volumes

Infrastructure

- Financial cloud servers are physically located in China
- Domestic hardware and SM-series cryptography are required for core banking
- Foreign cloud providers must partner with local firms

AI Governance

- Training data and algorithms require review and filing
- Models must run on certified domestic infrastructure
- Content labeling is required

Sources: China's PIPL (2021), Data Security Law (2021), Cybersecurity Law (2017, amended 2026). CAC Q&A Guidelines on Outbound Data Transfer Security Management (2025). Cross-border PI transfer framework updated March 2024 via "Provisions on Promoting and Regulating Cross-Border Data Flows" — raising thresholds and introducing FTZ exemption scenarios (Dacheng / JDSupra, December 2025).

CHAPTER 3 — CHINA

Macro Drivers for China's Framework

US–China Strategic Competition

- CHIPS Act, export controls, Trust Initiative
- 15th FYP self-sufficiency & substitution mandate, BRI

Dual-Track Approach

- Technological innovation + stringent state control
- The compliance regime grows more layered

Key Implications for JPMC

Departure from the “lowest common denominator”

- Increased R&D to deploy sovereign stack
- Data lake

Tech fragmentation resilience risk

- Expands attack surface
- Fined for resilience gaps & breaches

Structural regulatory conflict cannot be resolved

- CLOUD Act vs. DSL Article 36
- Structural IP exposure

Looking Ahead: 15th FYP (2026-2030) — **AI+ Action Plan, Data X Initiative**

What to Expect: Tighter localization mandates, escalated compliance costs

Sources: China's PIPL (2021), Data Security Law (2021), Cybersecurity Law (2017, amended 2026). CAC Q&A Guidelines on Outbound Data Transfer Security Management (2025). Cross-border PI transfer framework updated March 2024 via "Provisions on Promoting and Regulating Cross-Border Data Flows" (Dacheng / JDSupra, December 2025). King, Stubb & Kasiva, January 2026.

STRATEGIC ANALYSIS

Cross-Jurisdictional Conflict Matrix — Part 1 of 2

How EU, India, and China regulatory logic diverges across foundational and technical domains — and what it means for JPMC's operating model.

Each row is a compliance domain. The EU, India, and China columns show each jurisdiction's specific legal requirements. The JPMC Risk Exposure column translates regulatory divergence into concrete operational risk.

Subcategory	European Union EU	India IN	China CN	JPMC Risk Exposure
1. Regulatory Conflict	Rights-based sovereignty; GDPR, CRA, EUCS. Member-state variation (FR strict, DE technical).	Strategic interdependence; RBI, DPDP Act, SEBI. April 10, 2026 compliance deadline.	National security supremacy; CSL, DSL, PIPL, 15th Five-Year Plan. Party-state control.	Three incompatible sovereignty regimes require parallel compliance programs, costing hundreds of millions annually; no unified governance model is viable. ⚠ CRITICAL
2. Data Localization	Sector-specific mandates; financial data residency required for critical personal data.	Strict localization for financial & payments data; RBI mandates local storage.	Mandatory local storage for all important data; cross-border movement requires CAC approval.	Mandatory separate data stores in India and China raise TCO significantly. RBI barred Mastercard/AmEx for non-compliance — the same risk applies to JPMC. ⚠ HIGH
3. Cloud Architecture	EUCS Tier 3 certification Local audit trails	Sovereign Cell Architecture with local governance board Local HSMs mandatory	Ring-fenced domestic stack No global integration for classified systems Local data centers only	Three incompatible sovereign cloud architectures are required simultaneously Creating cross-border latency and heavy CAPEX The existing multi-cloud strategy must be rebuilt. ⚠ HIGH

STRATEGIC ANALYSIS

Cross-Jurisdictional Conflict Matrix — Part 2 of 2

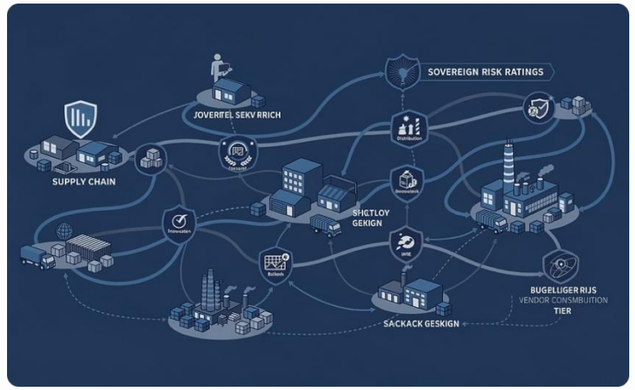
Subcategory	European Union EU	India IN	China CN	JPMC Risk Exposure
4. Third-Party	CRA vendor conformity requirements; mandatory exit strategies; annual vendor risk reviews.	RBI cloud outsourcing guidelines; vendor lock-in restrictions; domestic vendor preference.	Domestic vendors mandated for critical infrastructure; foreign vendor use restricted.	Hyperscaler reliance conflicts with China/India domestic vendor mandates; CRA enforces direct software liability and supply chain risks. ⚠ HIGH
5. AI Governance	CADA; High-risk classification for financial AI; explainability & human oversight mandatory.	SEBI algorithmic trading rules; AI model documentation required; no comprehensive AI law yet.	15th Five-Year Plan: domestic AI prioritized; foreign AI models subject to CAC security review.	China's domestic AI rules require separate pipelines and potential retraining of proprietary models. ⚠ HIGH
6. Business Continuity / Resilience	NIS2 Directive: ICT resilience & incident reporting; 4-hour initial notification; annual penetration testing.	RBI Business Continuity Policy; 2-hour RTO for payment systems; local DR sites required.	MLPS 2.0 resilience requirements; DR within China mandatory; no cross-border failover.	Incompatible RTO targets and China's cross-border failover ban force standalone resilience investment per jurisdiction, multiplying DR costs. ⚠ HIGH
7. Audit & Inspection Rights	DPAs and national competent authorities On-site audits possible GDPR Art. 58 & NIS2 Art. 32 supervisory & audit powers over ICT systems	RBI on-site inspections Data audit trails required Real-time reporting obligations	CAC and MPS have broad inspection authority Security assessment mandatory before data export	CAC/MPS unannounced inspection rights expose JPMC data to intelligence risk A single incident triggers simultaneous EU/India/China investigations, requiring three incompatible audit formats. ⚠ HIGH

Executive Takeaway

A one-size-fits-all compliance strategy will create recurring regulatory and operational failure points. The target state is a modular sovereignty architecture with different containment levels by market — EU sovereign regional zone, India portable sovereign cell, China domestic data island.

RECOMMENDATIONS

Recommendations — Part 1 of 2



Third-Party Risk

- EU Implement "sovereign risk ratings" for suppliers to mitigate systemic operational risks from supply chain divergence
- 🌐 Establish a technology sovereignty risk taxonomy to identify opportunities for cost-effective regulatory burden outsourcing to qualified third-party providers

Regulatory Conflict

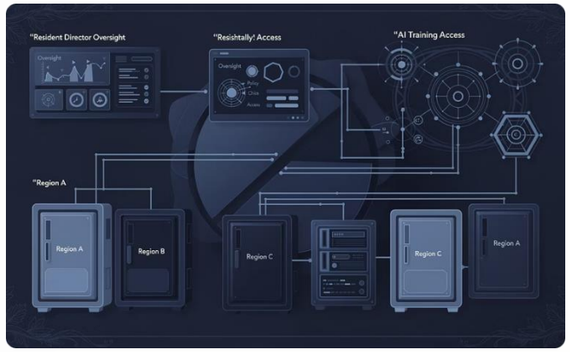
- 🌐 Improve coordination between regional, controls, and compliance teams to support preparedness and response protocols for conflicting sovereignty scenarios
- CN Standardize Hong Kong-based operations to PRC compliance standards to mitigate legal risks under the National Security Law

RECOMMENDATIONS

Recommendations — Part 2 of 2

Business Continuity

- CN Build a separate China technology stack on domestic infrastructure using Chinese encryption standards
- 🌐 Identify regulatory risk thresholds for when regulatory compliance costs outweigh market access gains



Data Localization

- IN Ensure resident veto: formally grant resident director veto power over global ”operational command center" changes to prevent jurisdictional breaches
- CN Run two parallel IP tracks: develop China-specific datasets, models, and algorithms for deployment on the China stack, and keep global proprietary IP out of the China perimeter entirely
- IN Activate sovereign AI nodes: leverage Pax Silica to deploy localized AI training clusters, ensuring models meet "explainability" requirements

The Effects of Deglobalization on Enterprise Technology

Geopolitical Pressure Continues to Rise

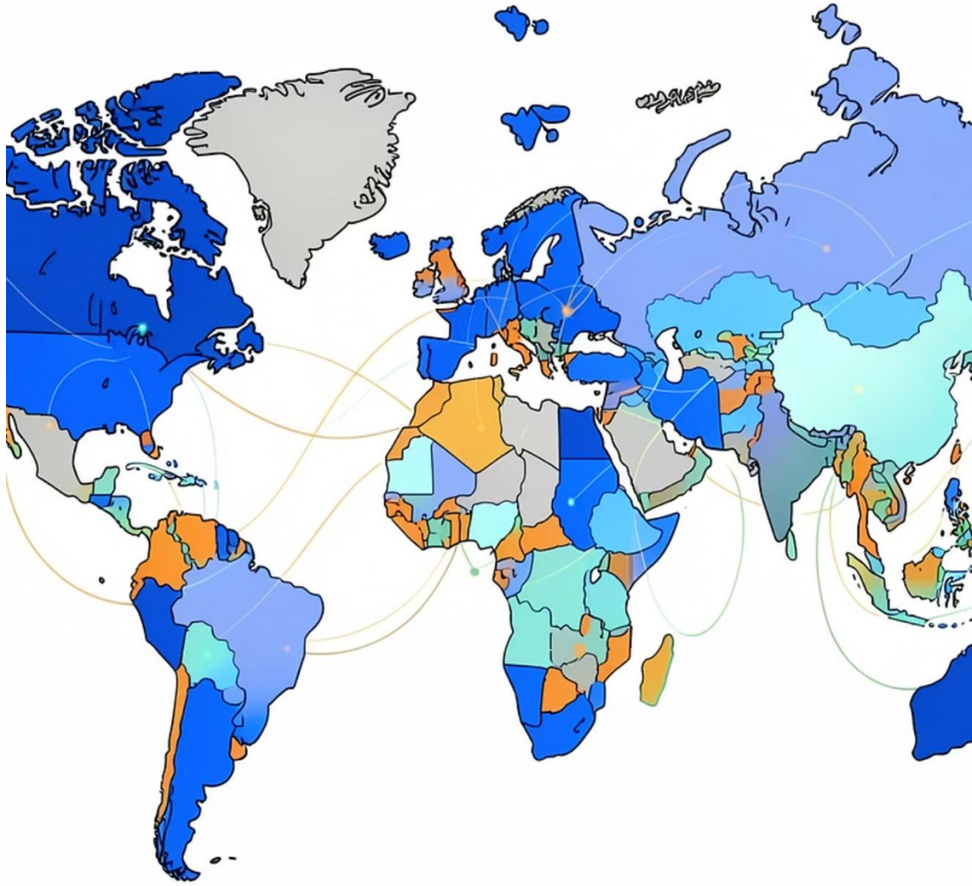
Stringent sovereignty mandates driven by geopolitical tensions and tightening data localization rules limit the use of key technologies. **JPMC's resilience planning should account for escalation**

The Lowest Common Denominator Model Under Stress

EU, Indian, and Chinese mandates are shaped by local politics and national objectives, creating a fragmented regulatory landscape for global firms. **JPMC should integrate local considerations into its global posture**.

Adapting to Complexity Costs Less Than Resisting It

Cumulative fines to ensure resilience, increasing market access costs, and technological restrictions across three strategic jurisdictions. **JPMC should invest today to maintain agility tomorrow**.



BIBLIOGRAPHY

Sources & References

Regulatory & Primary Sources

1. European Commission. (2024, December 10). *Cyber Resilience Act | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
2. European Union Agency for Cybersecurity (ENISA). (2024). *European cybersecurity certification scheme for cloud services (EUCS)*. https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
3. European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1732 amending Regulation (EU) 2021/1173 as regards the establishment of AI Factories*. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1732
4. Reserve Bank of India — Master Direction on Outsourcing of IT Services (RBI/2023-24/102, April 10, 2023). rbi.org.in
5. CAC (China) — Q&A Guidelines on Outbound Data Transfer Security Management (2025). cac.gov.cn
6. CAC (China) — Provisions on Promoting and Regulating Cross-Border Data Flows (March 2024).

Legal Analysis & Commentary

1. Exoscale — "CLOUD Act vs. GDPR: The Conflict About Data Access Explained" (October 21, 2025). exoscale.com
2. IndiaLaw LLP / Mondaq — "Building Compliance in the Cloud: RBI's IFS Cloud and the Future of Financial Data Localization under DPDPA 2023" (August 8, 2025). mondaq.com
3. King, Stubb & Kasiva / Mondaq — "DPDP Act Compliance for Physical and Digital Lending NBFCs" (January 21, 2026). mondaq.com
4. JSA / Mondaq — "RBI Master Direction on IT Outsourcing by Regulated Entities" (May 4, 2023). mondaq.com
5. Dacheng / JDSupra — "The Regulatory Framework for Cross-Border Personal Information Transfers in China: Latest Developments in 2025" (December 4, 2025). jdsupra.com
6. SLLS Law — "China's 2025 Data Transfer Regime: PIPL Compliance Blueprint for MNCs" (June 13, 2025). slls.law
7. AmCham China — "China's Evolving Data Security Framework for Financial Institutions." amchamchina.org
8. Program on International Financial Systems (PIFS) (Harvard Law) — "Data Localization, Cloud Adoption, and the Financial Sector" (July 2024). pifsinternational.org

All sources were accessed in February 2026. Citations reflect publicly available regulatory guidance and legal commentary. This briefing does not constitute legal advice.