International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 6, Nov – Dec 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Enterprise AI Data Sovereignty and Cross-Border Governance Framework

A Comprehensive Enterprise Framework for Governing AI Data Location, Jurisdiction, Residency, Transfer, Processing, and Cross-Border Risk

Sanjeeve Kumar Gajadi*
*(HCL Technologies, Bengaluru, Karnataka, India)
Email: sanjeevekumar.g@hcltech.com

****

Abstract:

Enterprise AI increasingly processes personal, confidential, regulated, and strategically sensitive data across global cloud regions, model providers, vector stores, data platforms, and agent tools. This creates data sovereignty challenges because data may be stored, transferred, inferred, logged, or processed across jurisdictions with different legal and contractual requirements. This paper proposes an Enterprise AI Data Sovereignty and Cross-Border Governance Framework that integrates data classification, jurisdiction mapping, residency controls, transfer mechanisms, provider due diligence, encryption, access control, logging, model restrictions, retrieval governance, and policy enforcement. The framework defines sovereignty zones, decision rules for model and region selection, cross-border risk scoring, data lineage, approval workflows, and continuous monitoring. It also addresses derived data, embeddings, prompts, model outputs, telemetry, fine-tuning data, and agent-mediated access. The proposed approach enables enterprises to scale AI globally while preserving legal defensibility, contractual obligations, business control, and data trust.

Keywords — Data Sovereignty, Cross-Border Data, AI Governance, Data Residency, Generative AI, Data Localization, Privacy, AI Security, Enterprise Architecture, Regulatory Compliance

****

I. INTRODUCTION

AI data flows are difficult to govern because prompts, retrieved content, embeddings, logs, model outputs, and tool interactions may cross technical and geographic boundaries.

Data sovereignty requires architecture decisions that reflect both where data is stored and where it is processed, accessed, replicated, or observed.

II. SOVEREIGNTY PRINCIPLES

Core principles include data minimization, purpose limitation, explicit jurisdiction awareness, least-privilege access, encryption, controlled transfer, and traceable processing.

Architecture should default to the most restrictive applicable requirement when legal or contractual obligations overlap.

III. DATA CLASSIFICATION AND JURISDICTION MAPPING

Data should be classified by sensitivity, ownership, residency requirement, transfer restriction, regulatory scope, and business criticality.

Jurisdiction maps should connect data classes with approved regions, providers, models, and processing patterns.

IV. SOVEREIGNTY ZONES

Enterprises can define sovereignty zones that group countries or regions with common processing rules and approved technical controls.

AI workloads should be routed only to zones that satisfy data classification and use-case requirements.

 ©IJSRED: All Rights are Reserved

V. CROSS-BORDER RISK SCORING

Risk scoring can consider sensitivity, destination jurisdiction, provider access, encryption, onward transfer, legal basis, retention, and reversibility.

High-risk transfers should require stronger approvals, contractual safeguards, and continuous monitoring.

VI. MODEL AND PROVIDER GOVERNANCE

Model providers should be assessed for data retention, training use, subcontractors, processing locations, support access, incident notification, and deletion commitments.

Enterprise policies should restrict providers that cannot meet required sovereignty or confidentiality controls.

VII. RAG AND VECTOR DATA GOVERNANCE

RAG architectures must govern source data, embeddings, vector stores, retrieval logs, and generated outputs.

Embeddings and derived representations should be treated according to the sensitivity of the source data when they can reveal or reconstruct protected information.

VIII. AGENTIC AI AND TOOL ACCESS

Agents may retrieve data from multiple jurisdictions and send results to external tools, creating indirect cross-border transfer.

Tool policies should enforce geography, data class, purpose, and recipient restrictions before execution.

IX. ENCRYPTION AND ACCESS CONTROL

Encryption in transit and at rest should be combined with customer-managed keys or regional key management where required.

Identity, role, purpose, and location-aware authorization reduce inappropriate cross-border access.

X. LINEAGE AND EVIDENCE

Data lineage should show source, transformation, embedding, retrieval, model processing, output, storage, and transfer locations.

Evidence should support internal audit, legal review, customer commitments, and regulatory inquiry.

XI. MONITORING AND POLICY ENFORCEMENT

Policy-as-code can prevent disallowed region selection, provider use, data movement, or tool invocation.

Continuous monitoring should detect configuration drift, unauthorized replication, cross-region logs, and new provider dependencies.

XII. CONCLUSION

The Enterprise AI Data Sovereignty and Cross-Border Governance Framework provides a structured method for controlling global AI data flows.

By integrating jurisdiction, architecture, identity, lineage, and policy enforcement, organizations can scale AI while preserving sovereignty, compliance, and enterprise trust.

ACKNOWLEDGMENT

The author acknowledges the contributions of enterprise architecture practitioners, AI governance specialists, security professionals, standards bodies, and technology researchers whose published work informed the concepts synthesized in this paper.

REFERENCES

[1] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), 2023.
[2] National Institute of Standards and Technology, AI RMF Generative Artificial Intelligence Profile, 2024.
[3] ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system.
[4] ISO 31000:2018, Risk management — Guidelines.
[5] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems.
[6] National Institute of Standards and Technology, SP 800-207: Zero Trust Architecture, 2020.
[7] The Open Group, TOGAF Standard, 10th Edition, 2022.

 ©IJSRED: All Rights are Reserved

[8] ISACA, COBIT 2019 Framework: Governance and Management Objectives, 2019.
[9] OWASP Foundation, OWASP Top 10 for Large Language Model Applications.
[10] MITRE, ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems.
[11] OECD, Recommendation of the Council on Artificial Intelligence.
[12] IEEE, Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems.

 ©IJSRED: All Rights are Reserved