CLARIA DATA SOVEREIGNTY CONSULTING SERVICE DEFINITION

Claria Data Sovereignty Consulting service helps organisations design and implement sovereignty-aware architectures, ensuring data stays where it should, under the right controls and in full alignment with your legal and operational obligations.

Core Service Offerings

- **Data residency assessments and risk audits:** We analyse and assess your current data landscape to identify where data is stored, processed and transferred, highlighting cross-border flows and exposure points.
- **Regulatory compliance alignment (GDPR, HIPAA, local data laws):** We assess your current practices against relevant national and industry-specific regulations, providing practical recommendations for alignment and enforcement.
- **Design of sovereign data architectures:** Architect and design systems and solutions that maintain critical data in your country.
- **Deployment in region-specific cloud and hybrid environments:** We implement data management and integration solutions within local or approved infrastructures, including sovereign cloud, private cloud and hybrid models.

- **Vendor selection and technology advisory for sovereignty compliance:** Robust framework and advisory service for vendor selection including commercial and technical assessments regarding sovereignty of data.
- **Policy and governance framework development:** Development of governance frameworks including policies and processes to enforce data sovereignty.
- **Sovereign data management solutions:** Claria have architected and developed integration, API management and data management solutions that are already data sovereign and ready to use.
- **Sovereign data management solutions:** Claria have architected and developed integration, API management and data management solutions that are already data sovereign and ready to use.

Engagement Model

Claria follows a structured, phased approach to move an organisation from a state of regulatory risk to one of jurisdictional control and strategic advantage. Depending on the nature of the engagement, some or all of the following may apply:

1. **Discovery & Assessment:**
    1. **Data Mapping:** Cataloguing where all critical datasets originate, where they are stored, and who accesses them across borders.
    2. **Maturity Audit:** Evaluating existing management practices against local laws like **GDPR**, the **US CLOUD Act**, or India's **DPDP**.
2. **Strategy & Framework Design:**
    1. **Data Categorisation:** Defining "sovereign data" categories (e.g., citizen IDs, financial records) that require strict local storage.
    2. **Policy Creation:** Establishing a **Data Sovereignty Policy (DSP)** that defines regional ownership and approval workflows for cross-border transfers.
3. **Architectural Implementation:**

    1. **Infrastructure Selection:** Guiding the move to Sovereign Cloud options or hybrid models that pin sensitive workloads to local regions.
    2. **Technical Controls:** Deploying **"Hold Your Own Key" (HYOK)** encryption and **Privacy-Enhancing Technologies (PETs)** to ensure only local authorities or owners can decrypt data.
4. **Operationalisation:**
    1. **Vendor Governance:** Auditing cloud partners and SaaS providers to ensure their disaster recovery (DR) sites and administrative access also comply with local laws.
    2. **Contractual Safeguards:** Implementing Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) for legal international transfers.
5. **Monitoring & Continuous Improvement:**
    1. **Compliance Dashboards:** Establishing real-time monitoring for unauthorized data egress or misconfigurations.
    2. **Periodic Reviews:** Quarterly assessments to stay aligned with rapidly evolving global regulations.