A powerful new force is reshaping the digital world: Digital Sovereignty

---

1. Introduction

Digital sovereignty refers to the ability of a state, organization, or individual to control and govern their own digital environment, rules, and destiny. In the Asia-Pacific (APAC) region, debates on digital sovereignty have intensified, expanding beyond technical issues to encompass geopolitical, economic, and security dimensions. This report synthesizes the slide presentation into a structured format to provide a comprehensive overview of digital sovereignty debates, data localization policies, business and national implications, and the broader geopolitical context in APAC.

---

2. Concept and Scope of Digital Sovereignty

Digital sovereignty is not synonymous with data localization. It encompasses **data sovereignty** (control over data) and **technological sovereignty** (strategic autonomy in technology). For instance, Korea's discourse on "AI sovereignty" highlights efforts to ensure independence in next-generation technologies.

---

3. Drivers of Data Localization in APAC

APAC countries are increasingly strengthening data localization measures due to:

- **National security and cybersecurity threats**
- **Economic competitiveness**
- **Regulatory autonomy**
- **Resilience and survivability**

Countries impose varying levels of restrictions on data storage, transfer, and processing, leading to diverse regulatory environments.

---

4. Country-Specific Data Localization Policies

Country	Regulations & Features	Data Localization Characteristics
Vietnam	Cybersecurity Law & Decree 53	Service providers must store user data domestically for at least 24 months

Country	Regulations & Features	Data Localization Characteristics
India	Digital Personal Data Protection (DPDP) Act 2023	“Blacklist” model allows cross-border transfers except to restricted nations; some sectors mandate localization
Korea	Requirements for public, financial, and healthcare sectors	Limited exemptions for AI-related overseas data processing
Indonesia	Personal Data Protection (PDP) Law	No explicit localization requirement
Australia	Privacy Act	Responsibility model: data breaches abroad hold companies accountable rather than enforcing localization

---

5. Business Implications of Data Localization

Data regulations significantly impact business operations by raising costs and limiting international activities. OECD findings indicate that storage and transfer restrictions increase ICT and legal costs. Some companies report that excessive restrictions could prevent them from operating internationally.

---

6. Strategies for Addressing Data Localization

Effective responses require:

1. **Avoiding one-size-fits-all approaches**: Tailored strategies for each context
2. **Country-specific regulatory analysis**: Understanding nuanced local requirements
3. **Flexible data architecture**: Leveraging multi-cloud and hybrid cloud strategies

The balance between privacy, security, economic growth, and cross-border data flows is essential.

---

7. Drivers and Debates around Digital Sovereignty

Key Drivers

- **National security and cybersecurity protection**
- **Economic competitiveness and reducing foreign dependency**

Debates

- What value does digital sovereignty create for APAC?
- Could it become a form of protectionism that harms regional digital economies?

---

8. Downsides of Digital Sovereignty

Strengthening digital sovereignty can also bring negative outcomes:

- Increased business costs
- Unequal burden on smaller nations
- Creation of trade barriers
- Digital fragmentation across regions

---

9. Cloud Strategies and the Rise of Sovereign Cloud

Growing concerns over data control, economic resilience, and geopolitical uncertainty have led to the emergence of the **“sovereign cloud”** model. This concept encompasses the entire digital architecture—data centers, communication infrastructure, and operational processes—and has become central to cloud adoption strategies.

---

10. Security and Sovereignty

Security and sovereignty are inseparable. Organizations dependent on outdated infrastructure that leaves data vulnerable to loss or theft cannot truly be considered sovereign.

---

11. Actionable Considerations

Digital sovereignty extends beyond data protection to encompass trust, economic ecosystems, and geopolitical resilience.

Dimension	Key Question	Detailed Considerations
Security & Control	Can I exercise more control over my data and operations?	Deploy supplementary data protection measures
Economic	Can I operate in an ecosystem based on trusted values?	Avoid lock-in and concentration risk from foreign providers
Geopolitical	How do I plan for disruptive scenarios amid instability?	Ensure survivability in case of forced disconnection

Google offers diverse models—public cloud, data boundary solutions, dedicated and connected cloud, and air-gapped cloud—to address varying regulatory and sovereignty needs.

---

12. Conclusion

The APAC debate on digital sovereignty reflects a dual reality: it supports security, economic growth, and technological independence while simultaneously raising business costs, creating trade barriers, and risking digital fragmentation. Policymakers must strike a balance between sovereignty and openness, while businesses need flexible architectures and multi-layered cloud strategies to adapt.