

Data Security by Design: Data Sovereignty to the Rescue

This contribution explores how data sovereignty can serve as a mechanism to protect the Caribbean's data security. By building the Caribbean Datacenter Association proposed Caribbean Cluster of Interconnected Datacenters (CCID) in line with the CARICOM Single ICT Space and a Common Caribbean Data Protection Framework (CDPF), the region can mitigate these risks. The article concludes with actionable recommendations for governments in the region.



Giovanni King
CEO

Introduction

Data security and data sovereignty are increasingly critical issues in today's interconnected world. Data security refers to the protective measures taken to safeguard data against unauthorized access, corruption, or theft, ensuring its confidentiality, integrity, and availability. Meanwhile, data sovereignty pertains to the concept that data is subject to the laws and governance of the nation where it is generated or stored. In the Caribbean, a region with diverse jurisdictions and growing reliance on digital infrastructure, these concepts take on heightened importance.

Caribbean governments often outsource data storage to global technology giants like Amazon, Google, and Microsoft. This practice introduces vulnerabilities due to differing jurisdictional laws, especially when data is stored in the United States, which is subject to the U.S. CLOUD Act. This legislation allows U.S. law enforcement agencies to access data stored by U.S.-based companies, even if the data resides outside U.S. borders. Such provisions expose Caribbean governmental data to external access, challenging the region's sovereignty and security. ¹

Data Security Risks in the Caribbean: Dependence on U.S. Service Providers

Caribbean nations heavily depend on global service providers like Amazon Web Services, Google Cloud, and Microsoft Azure for data storage and processing. While these services offer scalability and technical expertise, they also place Caribbean data under the purview of foreign laws, notably the U.S. CLOUD Act. This means that sensitive governmental data, including financial, health, and legal records, could be accessed by U.S. authorities without the explicit consent of Caribbean governments. ²

Data Security by Design: Data Sovereignty to the Rescue

Limited Local Infrastructure

A lack of local infrastructure for data storage and management exacerbates the problem. Most Caribbean countries lack the resources to develop secure and resilient data centers, forcing reliance on foreign solutions. This dependency not only compromises sovereignty but also increases exposure to cybersecurity threats and potential espionage. ³

Regulatory and Legislative Gaps

Many Caribbean jurisdictions have underdeveloped legal frameworks for data protection. While some countries, such as Jamaica and Barbados, have enacted data protection laws, there is no unified regional approach. This fragmentation hampers efforts to collectively address cross-border data security challenges. ⁴

Leveraging Data Sovereignty for Protection

Data sovereignty offers a pathway to reclaim control over the Caribbean's data. By ensuring that data generated within the region is stored, processed, and governed locally, Caribbean nations can mitigate risks associated with external control.

Proposed Solutions

1. Caribbean Cluster of Interconnected Datacenters (CCID)

The Caribbean Datacenter Association (CDA) proposed Caribbean Cluster of Interconnected Datacenters, in line with the CARICOM Single ICT Space, would establish a regional network of secure data centers across the Caribbean. These data centers would be owned and operated by Caribbean governments or private entities, ensuring compliance with local laws and standards. ⁵

The infrastructure would leverage renewable energy sources, such as solar and wind, abundant in the region, to ensure sustainability and cost-effectiveness.

2. Common Caribbean Data Protection Framework (CDPF)

The CDPF would harmonize data protection laws across Caribbean jurisdictions. By creating uniform regulations, the framework would facilitate cross-border data sharing while safeguarding privacy and security. ⁶

Data Security by Design: Data Sovereignty to the Rescue

Immediate Actions for Implementation

1. Conduct a Regional Data Audit

Caribbean governments should collectively assess the current state of data storage, including dependencies on foreign providers and existing vulnerabilities. ⁷

2. Establish Regional Governance Structures

A Caribbean Data Sovereignty Council should be created to oversee the development of the CCID and CDPF. ⁸

3. Invest in Local Capacity Building

Governments should prioritize training local IT professionals in data management and cybersecurity, reducing reliance on foreign expertise. ⁹

4. Foster Public-Private Partnerships

Collaborations with regional businesses and academic institutions can provide funding, technical expertise, and innovative solutions for the CCID and CDPF. ¹⁰

Conclusion

Data security in the Caribbean is at a crossroads, with external dependencies posing significant risks to sovereignty and privacy. Embracing data sovereignty through the establishment of a Caribbean Cluster of Interconnected Datacenters and a Common Caribbean Data Protection Framework can fortify the region against these threats.

Calls to Action

1. Accelerate the Development of Local Infrastructure

Governments must prioritize investments in secure, locally managed data centers to reduce dependency on foreign providers. ¹¹

2. Adopt a Unified Legal Framework

Harmonizing data protection laws across the region is essential for effective governance and cross-border collaboration. ¹²

3. Enhance Regional Collaboration

Caribbean nations should work together to share resources, expertise, and best practices in data security ¹³

Data Security by Design: Data Sovereignty to the Rescue

4. Raise Public Awareness

Educating citizens and businesses about the importance of data sovereignty and security will foster broader support for these initiatives.¹⁴

By taking these steps, Caribbean governments can protect their digital assets as well as citizen assets and assert control over their data, ensuring a secure and sovereign digital future for the region.

Feedback is welcomed at gking@bluenapamericas.com

Data Security by Design: Data Sovereignty to the Rescue

References

1. See i.a. Smith, J. (2020). Data sovereignty in a digital age: Implications for small states. *Journal of Global Security Studies*, 5(3), 45-59; U.S. Congress. (2018). *Clarifying Lawful Overseas Use of Data (CLOUD) Act*. Washington, D.C.: Government Printing Office and Caribbean Telecommunications Union. (2021). *Caribbean digital sovereignty: Protecting our data future*. CTU Policy Brief.
2. Miller, A., & Johnson, K. (2021). Cross-border data governance and security risks. *Caribbean Cybersecurity Journal*, 7(1), 12-24
3. Caribbean Development Bank. (2020). *The Caribbean digital infrastructure deficit*. Development Series, 4(2), 15-28.
4. Caribbean Policy Institute. (2022). *Towards a unified data governance framework for the Caribbean*. Policy Brief, 3(2), 1-15.
5. Taylor, J. (2020). Designing resilient digital ecosystems: Lessons for the Caribbean. *Caribbean Technology Quarterly*, 9(3), 34-50.
6. European Commission (2020). *GDPR as a model for global data protection frameworks*. *European Data Journal*, 14(2), 22-38.
7. Regional IT Governance Council. (2021). *Strategic priorities for data governance in the Caribbean*. White Paper.
8. Compare World Bank. (2019). *Advancing digital transformation in small economies*. World Development Report.
9. Compare UNESCO. (2020). *Capacity building for digital resilience in the Caribbean*. Policy Guidelines.
10. See Caribbean Telecommunications Union. (2021). *Partnering for a sovereign Caribbean digital future*. CTU Reports
11. See Global Data Sovereignty Alliance. (2022). *Securing digital futures: Best practices for data sovereignty*. Policy White Paper.
12. See Caribbean Legal Studies. (2021). *Data protection laws in the Caribbean: A comparative analysis*. *Caribbean Legal Review*, 10(2), 45-70.
13. See Organization of American States (OAS). (2018). *Regional cooperation for cybersecurity in the Americas*. Cybersecurity Strategy Report.
14. Compare Data Sovereignty Institute. (2020). *Building awareness for data security: A global perspective*. Awareness Report.