

ADVISORY

Legal Advice Note on a Data Embassy for Sint Maarten



ADOBESTOCK

Overview

This advice note, commissioned under a UN ECLAC Caribbean initiative, explores the feasibility, legal design, operational implications, and institutional prerequisites for establishing a “data embassy” for Sint Maarten. The concept of a data embassy entails placing a government-controlled, highly secure copy of critical national data and applications in a facility located outside the home territory but protected under treaty arrangements that confer inviolability and immunity—ensuring sovereignty over data even when stored abroad. The document is grounded in the Caribbean’s acute disaster-risk context and Sint Maarten’s specific constitutional, legal, and institutional realities as a country within the Kingdom of the Netherlands.

The document explains why digital continuity is now a matter of national resilience for small island states: essential public services, financial operations, identity and civil registration, and emergency management depend on digital systems that can be disrupted by catastrophic events. Using the pioneering Estonia–Luxembourg model as a benchmark, the note analyzes legal, diplomatic, technical, economic, and institutional dimensions and proposes a practical pathway for Sint Maarten to adopt a data embassy approach that safeguards digital sovereignty, continuity of government, and public trust.

Purpose and Audiences

The Caribbean’s exposure to hurricanes, floods, and seismic events creates systemic risks to core ICT infrastructure (data centers, power, and telecommunications). For Sint Maarten, Hurricane Irma underscored the risks to public service continuity and fiscal stability. The core problem the document addresses is how to secure the uninterrupted functioning of essential government systems in a small, disaster-prone jurisdiction with limited technical and institutional capacity. The shortcoming is twofold: (i) physical vulnerability of on-

island ICT assets and (ii) gaps in the legal and institutional framework to confidently host and govern government data extraterritorially, while ensuring privacy, security, and sovereignty.

The note aimed to advise Sint Maarten’s authorities on whether and how to establish a data embassy, and what legal, policy, and institutional measures are required to ensure digital sovereignty and continuity of critical services under disaster conditions. Primary audiences comprise policymakers and senior officials in the Government of Sint Maarten responsible for digital government, disaster risk management, legal affairs, and public finance. Secondary audiences comprise Kingdom of the Netherlands counterparts engaged in treaty/legal affairs; potential host-country officials; international partners and funders (e.g., UN ECLAC, World Bank); and legal and technical experts supporting digital resilience initiatives in the Caribbean.

What Is a Data Embassy?

A data embassy is a sovereign-controlled presence for critical government data and applications hosted abroad, protected by treaty-based inviolability and immunity from local jurisdiction, seizure, or interference. It allows a government to recover, operate, and deliver essential services even if domestic systems are compromised by disasters or other shocks.

There are two model variants: (i) treaty-backed physical facility (the “gold standard” per the note), drawing on the Estonia–Luxembourg precedent in a Tier III/Tier IV data center; and (ii) cloud-based or “virtual” models, which can be faster to deploy and cost-effective but may not provide equivalent legal sovereignty protections without strong legal instruments and controls. The key differentiators are legal status (inviolability, immunity), ownership and control of servers, encryption key management, and continuity procedures—including regular DR drills.

Context

Sint Maarten’s pursuit of a data embassy is shaped by legal, institutional, and operational constraints. As a constituent country within the Kingdom of the Netherlands, it cannot conclude treaties independently, requiring Kingdom coordination. Its outdated data protection framework and non-operational regulator weaken oversight and cross-border control, making legal modernization and treaty-based arrangements essential. Technically, the initiative must safeguard mission-critical systems through high-tier hosting, strong cybersecurity, defined DR and continuity targets, and open, modular architectures that preserve sovereignty and avoid vendor lock-in.

Key Findings

- **Feasibility:** A data embassy is feasible for Sint Maarten if accompanied by legal and institutional reforms and if implemented with a capable partner country under a carefully crafted treaty.
- **Legal necessity of a treaty:** To ensure inviolability and immunity comparable to diplomatic premises and archives, a binding international agreement is essential. Contractual terms alone—especially with commercial cloud providers—are insufficient to guarantee sovereignty.
- **Institutional readiness:** The lack of an operational data protection authority is a critical weakness; establishing or activating it is a priority to ensure oversight, public trust, and alignment with international standards.
- **Capacity constraints:** Given a population around 40,000 and limited technical resources, Sint Maarten will need strong partnerships for design, build, and operations, alongside a focused in-house unit to retain strategic control.

- **Comparative insight:** The Estonia–Luxembourg model offers a clear legal-technical benchmark; adapting it to a Kingdom structure and Caribbean risk profile will require tailored treaty design, governance, and financing solutions.
- **Economic context:** Post-disaster fiscal constraints elevate the importance of phased financing and leveraging external support (e.g., Kingdom, EU programs for OCTs, IFIs).

Risks, Constraints, and Mitigation Measures

The data embassy entails legal, political, economic, technical, and institutional risks that require targeted mitigation. Jurisdictional exposure is addressed through treaty-based inviolability, immunity, and sovereign control of encryption keys. Political and public risks are mitigated through inclusive engagement and transparent governance. Financial pressures call for phased, well-costed implementation, while technical risks require open standards, rigorous testing, and skills development. Institutional resilience could be mitigated by activating oversight authorities with clear accountability and audit mechanisms.

Lessons Learned

From Estonia’s experience:

- Treaty-backed physical facilities create the strongest legal shield for state data and systems.
- Diplomatic premises are not a technical substitute; purpose-built facilities with suitable tiering and controls are required.
- Regular drills and audits are indispensable—continuity is not an asset you purchase once, but a capability you practice.

For small island contexts:

- Clarity on which systems are truly mission-critical prevents scope creep and optimizes cost.
- Early, structured coordination with sovereign counterparts (in this case, Kingdom authorities) is essential to avoid legal dead-ends and delays.
- Building public trust requires visible regulatory capacity, transparent safeguards, and alignment with recognized standards (e.g., GDPR principles).

Strategic framing:

- Positioning the data embassy as an instrument of sovereignty and resilience—not outsourcing—helps secure political and public buy-in.
- Regional collaboration opportunities (e.g., shared learning or inter-operable standards) can reduce costs and strengthen collective resilience.

Recommendations

Policy and Legal

- Enact a National Ordinance (or comprehensive amendments) to establish a legal basis for digital government continuity, extraterritorial hosting under sovereign control, cybersecurity standards, and data lifecycle management.
- Align privacy and data protection rules with international standards (GDPR principles) to facilitate trust and partnerships.
- Engage early with Kingdom authorities to determine the most suitable legal instrument (e.g., Kingdom Act or treaty) that ensures inviolability and immunity for data embassy infrastructure and archives.

Institutional

- Activate and equip the Personal Data Protection Supervisory Committee to perform oversight, enforcement, and guidance functions.
- Establish a dedicated Digital Continuity Unit (or task force) with mandate over architecture, DR planning, vendor management, and exercises.
- Strengthen national cybersecurity arrangements, including CERT functions and incident response capabilities.

Technical and Operational

- Conduct a feasibility and prioritization assessment to identify mission-critical datasets and systems, define tiered RTO/RPO targets, and document dependencies.
- Architect the data embassy solution (networking, replication, security controls, access management) with attention to portability and lock-in avoidance.
- Plan and execute regular DR drills; embed continuity in procurement, SLAs, and governance processes.

Financing and Partnerships

- Develop a phased business case and financing plan; explore support from IFIs (World Bank, IDB), EU instruments relevant to OCTs, Kingdom resources, and responsible PPP structures.
- Identify and negotiate with potential host countries (e.g., Netherlands, Luxembourg, or other EU/friendly jurisdictions) for treaty-backed hosting with required technical standards.

Implementation Roadmap



Phase 1: Legal and Diplomatic Groundwork (Year 1)

- Draft and pass enabling legislation and/or ordinance updates.
- Engage Kingdom authorities to define legal pathways and commence treaty negotiations with target host(s).
- Activate the data protection authority and define regulatory guidelines for extraterritorial hosting and continuity.

Phase 2: Technical Design and Procurement (Years 1–2)

- Complete feasibility, critical systems mapping, and architecture design.
- Procure hosting arrangements, connectivity, and security tooling; finalize operational SLAs and audit provisions.
- Establish sovereign key management, access controls, and monitoring.

Phase 3: Deployment and Operationalization (Years 2–3)

- Migrate and replicate prioritized datasets; configure failover, conduct initial DR drills.
- Train staff; institutionalize playbooks and incident/continuity procedures.
- Conduct independent security assessments and readiness audits.

Phase 4: Steady-State Operations and Continuous Improvement (Ongoing)

- Schedule periodic DR exercises, audits, and penetration tests; update playbooks as systems evolve.
- Review legal and governance arrangements periodically; adapt to new risks and technologies.
- Expand scope incrementally (additional systems) based on performance and funding.

Governance, Roles, and Partnerships

Government of Sint Maarten	Policy lead; owner of the continuity program; responsible for legislation, architecture approval, and oversight of implementation.
Kingdom of the Netherlands	Diplomatic facilitation; legal authority for treaty-making; potential technical/financial support and expertise.
Host Country	Provision of treaty-backed legal status and secure data center environment.
Data Protection Authority	Oversight, compliance, enforcement, and guidance; public trust-building.
Technical Partners	Data center and telecom providers, cybersecurity firms, and advisory partners (including knowledge exchange with Estonia's e-Governance ecosystem).
Development Partners	Potential financing, technical assistance, and peer learning (e.g., World Bank, IDB, EU programs).

Methodology

This study adopts a four-phase, mixed-methods approach. Phase 1 maps baseline digital infrastructure, legal frameworks, and institutional arrangements. Phase 2 integrates hazard-impact and economic-loss considerations with legal and technical feasibility analysis of data embassy options. Phase 3 applies participatory co-design with stakeholders to identify practical solutions, barriers, and policy levers. Phase 4 conducts legal review and vetting, complemented by stakeholder validation to develop a consensus-based implementation roadmap.

Conclusion

A data embassy should be understood not merely as an IT project but as a sovereign capability integrating law, diplomacy, security engineering, and institutional governance. Treaty-based inviolability and immunity, reinforced by robust domestic legal reforms and an empowered regulator, form the foundation of durability. Success depends equally on disciplined governance, capacity building, and continuous practice, such as disaster recovery drills. Early, structured engagement with Kingdom authorities and a carefully sequenced, financed roadmap can translate the concept into an operational resilience asset.

This summary was produced with the assistance of an AI language model based on the original report. The full report is available at sintmaartenrecovery.org/analytical-studies