

Legal Advice Note on Data Embassies, Sint Maarten



**Sint Maarten - Data Embassies within
the UNECLAC Caribbean Initiative**

TABLE OF CONTENTS

Introduction	01
Background	03
Definition and Conceptual Foundations	04
Legal and Institutional Framework in Sint Maarten	05
Feasibility Analysis	07
Gaps and Risk Analysis	09
Recommendations and Roadmap	11
Conclusion	14



INTRODUCTION

The Caribbean’s prosperity and safety increasingly rest on digital assets—cloud platforms that host government registries, submarine cables that carry real-time payments, and data centres that power emergency-response dashboards. The very geography that drives tourism and maritime trade also exposes these assets to some of the world’s most destructive natural hazards. Over the past two decades, successive hurricanes, floods and earthquakes have demonstrated how a single severed cable or flooded server room can paralyse public-service delivery, shut down commerce, and impede humanitarian relief across entire island states.

Against this backdrop, the United Nations has commissioned a study to examine how the region can strengthen its digital backbone and guarantee service continuity when the next disaster strikes. The

mandate is precise: assess current vulnerabilities, model the potential economic and social losses of digital-infrastructure failure, evaluate the feasibility of “Data Embassy” arrangements, and produce actionable policy, legal, and investment recommendations for Caribbean governments and their partners. A Data Embassy—first popularised by Estonia—allows a nation to replicate its most critical data and applications in an extraterritorial facility that enjoys embassy-level sovereignty. For Small Island Developing States, hosting such replicas in a trusted jurisdiction outside the hurricane belt offers a unique path to safeguard continuity of government, financial markets, and essential social services even if domestic ICT facilities are destroyed.



To fulfil the terms of reference, the report adopts a mixed-methods approach across four phases. Phase 1 involves comprehensive data-gathering and baseline mapping (covering broadband density, data-centre capacity, and the regulatory and institutional frameworks for digital infrastructure). Phase 2 builds on this baseline with hazard-impact and economic-loss modelling to assess potential vulnerabilities. In parallel, a technical and legal feasibility review of the Data Embassy model is undertaken to determine its applicability and resilience in the regional context. Phase 3 focuses on identifying key structural and policy barriers to implementing secure and resilient digital infrastructure, through a participatory process of co-designing regionally tailored solution packages with stakeholders. Phase 4 involves legal review and vetting of proposed solutions, followed by stakeholder validation workshops to develop a consensus-driven roadmap for implementation (including any necessary regulatory and institutional reforms).

The results of these efforts are structured into the following components:

1. a quantified vulnerability and risk profile;
2. a region-specific feasibility assessment of Data Embassy models;
3. a synthesis of structural obstacles and pathways to resilient infrastructure;
4. an analysis of data sovereignty and cross-border legal issues;
5. a set of final policy, financing, and capacity-building recommendations designed to embed digital resilience at the heart of Caribbean disaster-preparedness strategies.

In short, the report will provide the evidence-based roadmap needed for Caribbean States to transform their digital infrastructure from a vulnerability into a resilient, sovereign asset capable of withstanding the region's growing climate threats.

Background

At the recent Ministerial Conference in Santiago of United Nations Economic Commission for Latin America and the Caribbean (ECLAC), which serves as the technical secretariat of eLAC: The Digital Agenda for Latin America and the Caribbean, countries in the region officially adopted the eLAC 2026 Agenda, which focuses on:

1. Expanding Digital Connectivity and Infrastructure
2. Enhancing Digital Security and Governance
3. Leveraging AI and Emerging Technologies for Development
4. Promoting Digital Inclusion and Skills Development
5. Modernizing Government and Public Services through Digital Transformation

To support the adoption of this agenda, working groups have been established to focus on specific areas. As part of this initiative, a new working group for the Caribbean has been inaugurated. This group is open to all independent nations of the Caribbean, as well as overseas territories. Additionally, digital transformation stakeholders are encouraged to apply for participation. Sint Maarten is part of the Working Group for the aforementioned Study.

Sint Maarten must navigate both its acute vulnerability to natural disasters and the accelerating digitalization of government services. As a Dutch Overseas Country and Territory (OCT) with a population of roughly 40,000, its economy and infrastructure are frequently tested by hurricanes and other extreme weather events. This not only threatens physical assets but also risks the loss or corruption of critical state data, from civil registries to financial systems. At the same time, Sint Maarten's legal architecture is characterized by overlapping responsibilities—local autonomy in internal matters alongside Kingdom-level control over foreign affairs—while its 2010 Data Protection Ordinance has yet to yield a fully operational supervisory authority.

In this context, the concept of a **data embassy**—an off-site, diplomatically protected data center treated under the home state's jurisdiction—offers a compelling solution for ensuring *digital continuity* of government functions even if domestic systems fail. First pioneered by Estonia after its 2007 cyber-attacks, the Estonian government and Luxembourg signed a bilateral agreement in 2017 to establish the world's first Data Embassy, granting inviolability and immunity to the servers holding Estonia's critical databases.¹ Today, data embassies are recognized as a strategic tool for small or disaster-prone states to safeguard sovereignty over their information assets, maintain uninterrupted public services, and bolster resilience against both natural and man-made crises.

This advice will guide Sint Maarten's policymakers through the legal foundations, feasibility considerations, and necessary reforms to implement a data embassy tailored to the territory's unique constitutional status and institutional capacities. It seeks to ensure that, come what may, the government's most vital data remains secure, accessible, and under Sint Maarten's sovereign control.

¹ <https://e-estonia.com/solutions/e-governance/data-embassy/>

1. Definition and Conceptual Foundations

- **Definition of Data Embassies:** A *data embassy* is essentially a secure data center located outside a nation's own territory but legally treated as an extension of that nation's sovereignty. The home state owns and controls server infrastructure abroad, and by special agreement the host state grants it protections akin to a diplomatic mission (inviolability from local jurisdiction, immunity from search/seizure).² In effect, the data embassy operates under the home country's jurisdiction even while on foreign soil.
- **Origin and Comparative Examples:** The concept was pioneered by Estonia as part of its digital continuity strategy. Following massive cyber-attacks in 2007³ and its move to a paperless government, Estonia sought a way to ensure government could continue operating digitally even if domestic IT systems were compromised. This led to the world's first data embassy: a bilateral treaty between Estonia and Luxembourg (signed 2017, ratified 2018) that established an Estonian-government-controlled Tier IV data center in Luxembourg.⁴ The Estonian data embassy serves as an off-shore backup for critical state databases (e.g., courts, land and business registers, population registry, etc.) while enjoying diplomatic-like immunity.⁵ Other nations are exploring similar concepts – for instance, Bahrain's 2018 "Cloud Law" allows foreign governments to store data in Bahrain's data centers under the foreign country's legal jurisdiction.⁶ These examples highlight different models for legally protecting off-shored data.
- **Strategic Importance in Modern Governance:** Data embassies are strategically valuable as a tool for national resilience. They ensure *digital continuity* of government operations in worst-case scenarios such as natural disasters, cyber warfare, or military invasion. By maintaining an up-to-date copy of crucial government information and services abroad, a country can continue serving its citizens even if its domestic infrastructure is crippled. This is especially pertinent for small or vulnerable jurisdictions – a data embassy provides disaster recovery, continuity of government, and protection against catastrophic data loss. Additionally, such external data centers can provide overflow computing capacity during peak needs (e.g. elections, tax filing season).⁷ In summary, the data embassy concept merges diplomacy, security, and IT strategy to bolster a nation's governance resilience in the digital age.

²<https://e-estonia.com/solutions/e-governance/data-embassy/#:~:text=not%20an%20embassy%20in%20the,physical%20embassies%20such%20as%20immunity>

³https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

⁴<https://e-estonia.com/solutions/e-governance/data-embassy/#:~:text=When%20we%20say%20%E2%80%9Cdata%20embassy%E2%80%9D%2C,physical%20embassies%20such%20as%20immunity>

⁵ *ibid.*

⁶ <https://www.lexology.com/library/detail.aspx?g=1498c8dc-5902-4f90-8a87-9c7eea170998>

⁷ Kotka, Taavi; Liiv, Innar (September 15, 2015). "Concept of Estonian Government Cloud and Data Embassies". In Kõ, Andrea; Francesconi, Enrico (eds.). *Electronic Government and the Information Systems Perspective*. Lecture Notes in Computer Science. Vol. 9265. Springer International Publishing. pp. 149–162. doi:10.1007/978-3-319-22389-6_11. ISBN 978-3-319-22388-9.

2. Legal and Institutional Framework in Sint Maarten

- **National Constitutional and Legislative Context:** Sint Maarten is a civil law jurisdiction and, since 2010, an autonomous country within the Kingdom of the Netherlands. It has its own Constitution (Staatsregeling) and legal system, largely inherited from the former Netherlands Antilles. Domestic governance is fully autonomous *except* for certain “Kingdom affairs” like defence, foreign relations, and citizenship which remain the responsibility of the Kingdom government.⁸ This division means that while Sint Maarten can legislate on internal matters (such as data management or privacy), any international agreements (e.g., a treaty to establish a data embassy with another state) would likely involve the Kingdom’s oversight or consent due to foreign affairs being a Kingdom prerogative.

Notably, the Constitution of Sint Maarten enshrines fundamental rights including privacy; for example, it guarantees respect for personal privacy (in line with European human rights conventions) and anticipates that detailed privacy protections will be provided by national ordinance.⁹ Thus, the constitutional backdrop supports data protection principles, which are elaborated through legislation.

- **National Ordinance on Data Protection (2010):** The primary data protection law is the **National Ordinance for the Protection of Personal Data** (Landsverordening bescherming persoonsgegevens), effective since the 10 October 2010 constitutional change (published as AB 2010, no. 2).¹⁰ This Ordinance provides a legal framework for personal data processing in Sint Maarten. It sets out general principles governing the collection, use, and disclosure of personal information and grants individuals specific rights over their data.¹¹ For instance, under this law personal data may only be processed on legitimate grounds – such as with the individual’s unambiguous consent or for compliance with legal obligations or public tasks. The Ordinance also imposes duties on data controllers (e.g., government agencies) regarding data security and accountability, and includes provisions for liability and sanctions in cases of data misuse.¹² Importantly, the 2010 Ordinance created an oversight body, the *Personal Data Protection Supervisory Committee*, mandated to supervise and enforce the data protection rules.¹³ This committee was intended to function as an independent data protection authority for Sint Maarten. However, in practice, this supervisory authority has not yet become fully operational (the law stipulates its establishment, but as of now the committee either remains unstaffed or is not effectively enforcing compliance). The absence of an active data protection authority is a significant institutional gap in

⁸<https://www.doingbusinessdutchcaribbean.com/st-maarten/introduction-sxm/constitution-governance-sxm/#:~:text=Apart%20from%20certain%20affairs%20that,European%20Community%20as%20a%20whole>

⁹https://sintmaartengov.org/Documents/Translated%20Legislation/AB%201_MvT%20Staatsregeling.pdf#:~:text=fundamental%20rights%20are%20included%20in,or%20the%20environment%2C%20or%20for

¹⁰<https://btp.sx/f/Publishing/2018-06-06/10t98470905491#:~:text=%EF%81%B5%20GDPR%20does%20not%20apply,committee%20will%20have%20the%20responsibility>

¹¹<https://thinktodoinstitute.com/wp-content/uploads/2024/03/T2DI-National-Data-Maturity-Research-2024.pdf#:~:text=As%20for%20Cura%C3%A7ao%2C%20the%20National,it%20is%20necessary%20for%20compliance>

¹²<https://thinktodoinstitute.com/wp-content/uploads/2024/03/T2DI-National-Data-Maturity-Research-2024.pdf#:~:text=As%20for%20Cura%C3%A7ao%2C%20the%20National,it%20is%20necessary%20for%20compliance>

¹³<https://www.theinformationcollective.com/dpl/sint-maarten-nederlands#:~:text=1,Committee%20which%20is%20responsible%20party%C2%A0for>

the current framework (discussed further in Section 4).

- **Role of the Kingdom in Foreign Affairs and Treaties:** As noted, foreign relations are a Kingdom affair. This has two key implications. First, any treaty or formal agreement with another country to host a “data embassy” for Sint Maarten would require coordination with (and likely the assent of) the Kingdom government (the Netherlands on behalf of the Kingdom).¹⁴ In practical terms, while Sint Maarten’s local government can initiate and negotiate aspects of such an arrangement, the Kingdom’s involvement is necessary for the international legal formalization. Second, the Kingdom’s existing treaty relationships and memberships could influence Sint Maarten’s options. For example, the Kingdom of the Netherlands could potentially facilitate arrangements by extending its diplomatic privileges or by including Sint Maarten in relevant multilateral frameworks.

However, it also means Sint Maarten alone cannot unilaterally guarantee foreign diplomatic status to its data center without a Kingdom-level instrument. Any plan for a data embassy must therefore fit within the Kingdom’s constitutional structure – possibly via a Kingdom Act or a bilateral treaty to which the Kingdom is a party. Policymakers must account for this in crafting the legal strategy for a data embassy.

- **Applicability of GDPR and International Standards:** Unlike the European Netherlands, Sint Maarten is **not** part of the European Union, so the EU’s General Data Protection Regulation (GDPR) does not directly apply.¹⁵ Sint Maarten relies on its own 2010 Data Protection Ordinance for privacy regulation. That said, international standards still play a role. The GDPR’s extra-territorial reach means that Sint Maarten-based entities (including possibly government services) must comply with GDPR if they offer goods or services to EU residents or monitor their behaviour.¹⁶ Moreover, the island’s northern half, Saint-Martin, is an EU territory governed by French law, placing Sint Maarten in a distinctive position where some of the world’s most stringent data protection standards—such as the GDPR—are enforced just across a shared border. Thus, Sint Maarten’s data practices operate in the shadow of European standards. In developing a data embassy, alignment with global best practices (EU GDPR principles, Council of Europe Convention 108+, etc.) would bolster credibility and interoperability. Ensuring EU-equivalent data protection measures will be crucial if the chosen host country is in Europe or if EU citizen data might be stored. Finally, while GDPR doesn’t automatically cover Sint Maarten, the local Ordinance was modelled on earlier European privacy frameworks and shares similar concepts. Modernizing Sint Maarten’s data protection regime in light of the GDPR (for example, incorporating stricter requirements for data transfers, breach reporting, etc.) could be a strategic move as part of the data embassy initiative – ensuring alignment with high international

¹⁴<https://www.doingbusinessdutchcaribbean.com/st-maarten/introduction-sxm/constitution-governance-sxm/#:~:text=Apart%20from%20certain%20affairs%20that,European%20Community%20as%20a%20whole>

¹⁵<https://btp.sx/f/Publishing/2018-06-06/10t98470905491#:~:text=%EF%81%B5%20GDPR%20does%20not%20apply,committee%20will%20have%20the%20responsibility>

¹⁶<https://www.dlapiperdataprotection.com/index.html?t=law&c=SX#:~:text=Ordinance%20Personal%20Data%20Protection%E2%80%9D%29%3B%20,behaviour%20in%20the%20European%20Union>

standards and enabling necessary data-sharing agreements.

3. Feasibility Analysis

- **Administrative and Technical Capacity:** A realistic appraisal of Sint Maarten's administrative and IT capacity is essential. Implementing a data embassy is a complex endeavour requiring robust digital infrastructure, cybersecurity expertise, and 24/7 operational monitoring. As a small island government (population ~40,000) with constrained resources, Sint Maarten may currently lack the full in-house capacity to deploy and manage a sovereign data center abroad. The fact that its data protection supervisory committee has remained inactive suggests limitations in institutional capacity within the data governance domain.¹⁷ There is also a question of technical manpower – skilled ICT personnel and redundancy plans are needed to maintain a secure backup site. Policymakers should assess what existing e-government systems and data management protocols are in place domestically.

The government's IT apparatus might need strengthening (or outsourcing partnerships) to handle the encryption, replication, and protection of sensitive data in transit and at rest. On the positive side, establishing a data embassy could be leveraged to attract investment in modernizing local IT infrastructure as well. In summary, while feasible, the project would likely require capacity-building measures – such as training, dedicated budget for ICT upgrades, and possibly support from international partners or private contractors for the technical build-out.

- **Sovereignty, Jurisdictional Control and Data Localization:** By design, a data embassy must remain under Sint Maarten's legal control despite being physically abroad. This raises core questions of sovereignty and jurisdiction. The feasibility depends on negotiating a legal arrangement wherein the host country recognizes the extraterritorial status of Sint Maarten's servers and data. In practice, this means the data embassy premises would need to be declared *inviolable* – the host authorities would have no right to enter, search, seize or interfere with the equipment or data without Sint Maarten's consent.¹⁸ Ensuring this level of control typically requires a binding bilateral agreement (akin to a treaty) that grants immunity to the data center (much as embassies and their archives are protected under the Vienna Convention).¹⁹ Without such guarantees, any data stored abroad could be subject to the host country's jurisdiction and vulnerable to subpoenas or surveillance by the host's agencies – an unacceptable risk. Thus, jurisdictional clarity is a make-or-break aspect: Sint Maarten must either choose a partner willing to codify these protections (as Luxembourg did for Estonia) or alternatively pursue hosting within a jurisdiction that already accords special status (for example, within the Kingdom or a trusted ally). Data localization laws also come into play. Sint Maarten currently has no strict data localization requirement forcing government data to stay on-island, but the spirit of sovereignty implies critical

¹⁷ *ibid.*

¹⁸ <https://www.diplomacy.edu/blog/data-embassies-protecting-nations-in-the-cloud/#:~:text=against%20cyberattacks%20is%20the%20data,state%20and%20the%20receiving%20state>

¹⁹ *ibid.*

state data should remain under national jurisdiction. A data embassy, if properly structured, satisfies localization concerns by extending national jurisdiction to foreign soil. Policymakers must be prepared to address legal questions such as which country's laws govern access to the data, how to manage potential conflicts of law, and how to enforce data protection obligations when servers are located abroad. Careful treaty drafting and possibly new local legislation will be needed to cement Sint Maarten's jurisdictional control over its extraterritorial data holdings.

- **Disaster Resilience and Continuity of Government:** A primary motivation for a data embassy is to bolster disaster resilience. Sint Maarten is acutely aware of natural disaster risks – for example, Hurricane Irma in 2017 devastated infrastructure and underscored the vulnerability of on-island facilities. Off-island backups of critical data can ensure continuity of government operations after such catastrophes. Feasibility in this regard involves identifying what core government databases and services are *mission-critical* and planning for their replication in the data embassy. This includes civil registries, property and cadastral records, financial management systems, and possibly even e-government services (so that the public can access essential services remotely if local systems are down).

The technical feasibility of real-time or near-real-time data synchronization must be evaluated given bandwidth and connectivity constraints (Sint Maarten would need a secure, high-speed network link to the host data center, potentially via dedicated submarine cable or satellite backup, to transmit updates and to failover services during an emergency.) As seen in Estonia's case, a data embassy enables the government to continue functioning digitally even if the national territory is compromised. For Sint Maarten, which faces recurring hurricanes and is geographically small, the continuity benefit is significant. Moreover, a data embassy could be part of a broader national disaster recovery plan, complementing other measures like hardened local data centers or cloud backups. In terms of feasibility, the government must ensure it can operationalize a switchover to the data embassy during a crisis (i.e., employees know how to access systems remotely, data is up-to-date, and applications can run from the foreign site). Planning and drills would be advisable. Overall, investing in a data embassy greatly enhances resilience, but it also requires a commitment to maintain off-site systems and integrate them into the country's emergency response strategy.

- **Physical vs. Virtual Embassy Infrastructure:** Policymakers should consider what form the data embassy will take. One option is a **physical** data embassy – i.e., dedicated server hardware housed in a secure facility abroad, established via a diplomatic agreement. This was the route Estonia chose: rather than using existing embassy buildings, they set up servers in a specialized Tier IV data center for maximum security and uptime.²⁰ Notably, Estonia initially explored converting some of its traditional embassies (diplomatic missions) into data embassies, but decided against it because standard embassy premises lacked the requisite technical infrastructure and disaster resilience (they weren't built to data-center specifications

²⁰<https://e-estonia.com/solutions/e-governance/data-embassy/#~:text=When%20we%20say%20%E2%80%9Cdata%20embassy%E2%80%9D%2C,physical%20embassies%20such%20as%20immunity>

and depended on local telecom networks). This insight suggests that a purposefully built or professionally hosted data center is preferable over a makeshift server room in an office. The other possibility is a **virtual** data embassy, for example using a *cloud-based* solution. A public cloud (like AWS or Azure) distributed across multiple locations would provide redundancy, but it cannot easily confer sovereign immunity or exclusive jurisdiction to Sint Maarten. Without a physical footprint to treat as diplomatic premises, purely cloud approaches raise legal uncertainties – the data would be subject to the provider’s jurisdiction and terms of service. A middle ground could be a *private cloud* or a leased cage in an existing data center, combined with a legal agreement to treat that environment as sovereign. In summary, the feasibility analysis should weigh these models: a **treaty-backed physical data embassy** (high control and security, but higher cost and complexity) versus a **contractual cloud solution** (potentially lower cost and scalable, but with weaker legal protections). For the purpose of true sovereignty and long-term assurance, the physical/treaty model is likely the only option that meets the stringent requirements of a “data embassy.” This will entail identifying a host facility that meets top security standards (redundant power, cooling, cyber defences, etc.) and negotiating the necessary immunity for that site.

4. Gaps and Risk Analysis

- **Legislative and Institutional Gaps:** A review of Sint Maarten’s current laws and institutions reveals several gaps that must be addressed before a data embassy can be realized.

Legislative gaps: The existing data protection ordinance (2010) predates modern developments and does not explicitly contemplate government data being held extraterritorially. There is no current law or policy on “data sovereignty” or digital continuity that would authorize, govern, or regulate a data embassy arrangement. Provisions on cross-border data transfer in the 2010 Ordinance (inspired by older EU directives) are likely inadequate for this scenario – they may permit transfers given certain privacy safeguards, but they do not equate to establishing a permanent foreign data repository under local jurisdiction. New or amended legislation is needed to fill this void (see Section 5).

Institutional gaps: Perhaps the most glaring is the absence of an effective data protection authority. Although the law provided for a Personal Data Protection Supervisory Committee, it has not been functioning.²¹ This means there is currently no independent regulator to oversee data privacy or security either in general or for a sensitive project like a data embassy. Additionally, there may be gaps in overall cybersecurity governance – for instance, Sint Maarten may not yet have a dedicated national cyber security strategy or a CERT (Computer Emergency Response Team) that could be involved in safeguarding a data embassy. Without strong institutions, the risks of mismanagement or regulatory non-compliance increase. Strengthening or

²¹<https://btp.sx/f/Publishing/2018-06-06/10t98470905491#:~:text=%EF%81%B5%20GDPR%20does%20not%20apply,committee%20will%20have%20the%20responsibility>

establishing the necessary bodies (data authority, IT security units) is crucial to mitigate these gaps.

- **Cross-Border Legal Challenges:** Hosting government data abroad introduces complex legal challenges, especially if not meticulously structured. One risk is exposure to foreign legal processes: without an immunity arrangement, courts or law enforcement in the host country (or even third countries) might attempt to subpoena or seize Sint Maarten's data under their laws. For example, data stored in a foreign jurisdiction could be subject to search warrants from that jurisdiction, undermining the confidentiality of sensitive information. A well-documented concern is foreign surveillance – intelligence agencies might target the data centre's communications or exploit legal avenues (like the U.S. CLOUD Act, if data were in the U.S.) to access the data. Nations have their own national security and law enforcement mandates, which could conflict with Sint Maarten's desire to keep its data sovereign. Another challenge is conflict of laws: personal data in the embassy might include information about individuals from various nationalities (e.g., EU citizens residing or doing business in Sint Maarten). This raises questions about which data protection laws apply – Sint Maarten's, the host country's, or even EU law – and how to resolve disputes. There is also the issue of **data transit**: data traveling to and from the embassy could pass through multiple jurisdictions (cables, routers in other countries), potentially subject to interception or differing legal regimes. Lastly, any arrangement must consider **termination or dispute scenarios** – if relations with the host country deteriorate or if a legal dispute arises (say, a host country court order conflicting with Sint Maarten's laws), how will it be handled? To address these risks, the legal framework of the data embassy must clearly establish that the data remains under Sint Maarten's jurisdiction and is *inviolable* by the host state. Additionally, strong encryption and network security are needed to mitigate surveillance and interception risks. The success of a data embassy is heavily dependent on mutual trust and clarity between Sint Maarten and the host state; any ambiguity in the agreement could become a serious vulnerability.
- **Political and Economic Risks:** Beyond purely legal issues, there are political and financial considerations.

Political risks: The data embassy concept requires sustained political will and stability. Government turnover or shifting priorities in Sint Maarten could stall or reverse such an initiative, especially if it's not broadly understood by policymakers or the public. There may be sensitivity about placing national data in foreign hands – some stakeholders could perceive it as ceding control or might distrust the chosen host country. It is essential to build consensus and public confidence that a data embassy reinforces—rather than undermines—national sovereignty. Diplomatically, choosing a host nation must be done carefully to avoid geopolitical entanglements; aligning with one partner (say, the Netherlands or another European State) might have implications for relations with others.

Economic and funding risks: Sint Maarten's budget is under strain, especially in the wake of disaster recovery needs (the government faced a major deficit after Hurricane

Irma, roughly \$230 million by 2019).²² Investing in a state-of-the-art data embassy (with ongoing operational costs) will compete with other urgent funding priorities. There's a risk that the project could be under-funded or delayed if economic conditions worsen or if donor support doesn't materialize. Moreover, the long-term sustainability must be considered – will there be funds to regularly upgrade equipment, maintain security standards, and train personnel? Another economic risk is over-reliance on external vendors: if the technical solution is outsourced, the government might face vendor lock-in or escalating costs.

Mitigation: These risks can be managed by securing external funding grants (for example, from EU development funds or the World Bank for climate/digital resilience), and by treating the data embassy as a phased project with clear milestones and cost-benefit analysis. Politically, early engagement with key decision-makers and the community to explain the benefits (e.g., how it protects citizens' data and government continuity) can build the necessary support. It may also help to frame the initiative as part of a broader national development in ICT and innovation, thereby aligning it with positive nation-building narratives.

5. Recommendations and Roadmap

Legal Reforms and Framework: It is recommended that Sint Maarten begin by updating its legal framework to explicitly enable and regulate the establishment of a data embassy. This could be achieved either through the enactment of a dedicated National Ordinance on Digital Government Continuity or by amending the existing 2010 Data Protection Ordinance to address issues such as cross-border data hosting, jurisdiction, and emergency access protocols.

Key legal elements should include: provisions that authorize the government to enter into agreements for off-shore data storage; rules for classifying which data can be replicated to a foreign site; data transfer safeguards (encryption, access controls, compliance with privacy principles); and recognition of the extraterritorial status of the backup (perhaps referencing that it shall be treated akin to diplomatic premises under the Vienna Convention rules).²³ In parallel, any such law should address data sharing between Sint Maarten and the host state, and lay out accountability (e.g., requiring periodic audits of security). Given the Kingdom context, consider whether a **Kingdom Act** or consensus Kingdom law is needed to facilitate cooperation with Dutch institutions – for instance, if leveraging Dutch expertise or infrastructure (this has been a topic of debate in other areas of law).²⁴ It may be prudent to consult Kingdom partners early and, if possible, design the legal instrument to allow extension to Aruba and Curaçao as well (a regional approach could have benefits if multiple Dutch Caribbean countries pursue similar digital continuity measures). Additionally, align new regulations with international standards – for example, incorporate GDPR-level

²²<https://nrpbxm.org/wp-content/uploads/2019/08/NRRP.pdf#:~:text=Fiscal%20Challenges,to%20finance%20budget%20deficits%20between>

²³<https://www.diplomacy.edu/blog/data-embassies-protecting-nations-in-the-cloud/#:~:text=the%20Vienna%20Convention%20on%20Diplomatic,VCDR>

²⁴<https://thinktodoinstitute.com/wp-content/uploads/2024/03/T2DI-National-Data-Maturity-Research-2024.pdf#:~:text=Since%202019%2C%20the%20scope%20and,on%20the%20implementation%20of%20a>

protections for personal data in the data embassy, to ease any data exchange with European entities.

- **Institutional Developments (Capacity Building):** Strengthening institutions is critical for implementation. **Activate the Data Protection Authority:** Priority should be given to establishing the Personal Data Protection Supervisory Committee. This body will be essential to oversee compliance, handle any privacy concerns related to the data embassy, and reassure both local and international stakeholders that Sint Maarten takes data governance seriously.²⁵ Steps may include allocating budget, appointing qualified members (perhaps with some outside experts or exchange with the Dutch Autoriteit Persoonsgegevens for training), and empowering the authority to issue guidelines relevant to government data storage. **Create a Dedicated Digital Continuity Unit:** The government might set up a specialized unit or task force for the data embassy project – bringing together IT staff, legal advisors, and disaster recovery planners. This unit would manage the technical rollout and be the liaison with the host country’s technical teams. It should also develop operational protocols (for data backup frequency, failover procedures, etc.). **Cybersecurity and IT infrastructure:** possibly establish a national Computer Emergency Response Team (CERT) if one doesn’t exist, or enhance the National ICT Department’s security capabilities, to monitor and defend the data flow between Sint Maarten and the embassy. **Training and awareness:** It’s recommended to train civil servants in how to use the continuity systems (e.g., how to access government applications via the data embassy if the main systems are down). Building local capacity ensures long-term self-reliance rather than complete dependence on foreign contractors.
- **International Cooperation Options:** Explore and pursue cooperative arrangements to support the data embassy. One route is a **bilateral treaty** with a specific country willing to host the data center under agreed terms (much like Estonia-Luxembourg). Potential host partners might include the Netherlands (given the close constitutional ties and existing trust) or another friendly nation with advanced infrastructure (for example, Luxembourg has experience in this concept, or an EU state that might be interested in digital cooperation). Working through the Kingdom’s diplomatic channels will be necessary to formalize any such agreement. Another avenue is **multilateral cooperation** – Sint Maarten could seek to participate in EU or international programs for digital resilience. As an Overseas Country and Territory (OCT) associated with the EU, Sint Maarten might access EU funding or technical assistance for projects enhancing cybersecurity and data management. Partnering with organizations like the Estonian e-Governance Academy or the OECD could provide guidance; knowledge exchange with Estonia or other pioneers could help in crafting the right approach. Also, consider **regional partnerships:** perhaps collaborate with other Caribbean nations on a joint backup facility (although sovereignty issues would need careful handling, a shared Caribbean digital continuity center under joint governance might be proposed in the long term). If internal capacity is limited, Sint Maarten might even negotiate for temporary use of an ally’s secure cloud with an MOU in place, as an interim step. The

²⁵https://btp.sx/dash/files/Publishing/2018-06-06/10t98470905491___UHJlc2VudGF0aW9uIEtleSBOb3RIIFNwZWFrZXI=b_64.pdf#:~:text=%EF%81%B5%20GDPR%20does%20not%20apply,committee%20will%20have%20the%20responsibility

overarching recommendation is to secure a host environment that is stable, secure, and backed by a clear legal instrument guaranteeing Sint Maarten’s ownership and control of the data.²⁶ This likely means formalizing an agreement that explicitly grants the data embassy immunity from local jurisdiction and defines cooperation protocols (e.g., how law enforcement requests are handled, if at all). Early diplomatic engagement should be initiated to identify the best cooperation mechanism – whether through Kingdom facilitation or direct bilateral talks.

- **Funding and Technical Implementation Pathways:** Develop a phased roadmap for implementation, coupled with a financing plan. **Funding:** Identify sources of funding such as: the World Bank and IDB (which have shown interest in Caribbean digital infrastructure and disaster resilience), EU funding under OCT initiatives, Kingdom government support (the Netherlands may co-finance certain capacity-building aspects as part of broader reconstruction or digitalization aid), or public-private partnerships with tech firms. Preparing a solid business case – emphasizing how a data embassy protects not just government functions but also investor confidence and economic stability – can help unlock these funds. **Technical implementation:** Start with a pilot or feasibility study. For example, conduct an assessment of current data assets and determine which datasets should be prioritized for backup. Next, work with ICT consultants to design the architecture: this includes choosing the physical data center location (ensuring it meets Tier III+ standards for reliability), planning secure communication links (possibly dedicated VPN or encrypted lines), and selecting technologies for data replication (e.g., real-time database mirroring, secure cloud storage appliances, etc.). Employ state-of-the-art encryption (both in transit and at rest) so that even if data were intercepted, it remains unreadable.

Consider using innovative integrity solutions like blockchain hashing for critical records (notably, Estonia’s data embassy uses KSI blockchain to ensure data integrity against tampering).²⁷ The implementation plan should also outline **testing and maintenance:** e.g., schedule regular disaster recovery drills where the government simulates switching over to the overseas backup, to validate that services can run from there in an emergency. Over time, scale up the system – perhaps starting with backing up less sensitive archives first, then moving to live critical systems once confidence and security are proven. **Timeline:** Set short-term (1 year) goals like legal preparations and partner selection, medium-term (2–3 year) goals like building and commissioning the data embassy, and long-term ongoing tasks like updates and audits. Throughout, ensure transparency and include the Data Protection Authority in approvals to maintain compliance with privacy obligations. By following a clear roadmap with political support, technical expertise, and secure funding, Sint Maarten can realistically achieve a functional data embassy in the coming years.

²⁶<https://e-estonia.com/solutions/e-governance/data-embassy/#:~:text=not%20an%20embassy%20in%20the,physical%20embassies%20such%20as%20immunity>

²⁷<https://e-estonia.com/solutions/e-governance/data-embassy/#:~:text=is%20an%20innovative%20concept%20for,are%20capable%20not%20only%20providing>

In conclusion, establishing a data embassy for Sint Maarten is a forward-looking initiative that can significantly strengthen the nation's resilience and sovereignty in the digital era. This advice has identified the foundational concept and its benefits – chiefly, ensuring continuity of government operations and safeguarding vital data against local disruptions. It has examined Sint Maarten's legal context, noting the existing data protection framework (2010 Ordinance) and the need to update laws and institutions to meet this new challenge. The feasibility assessment highlighted that while there are capacity constraints and complex jurisdictional issues, these can be overcome through careful planning, international cooperation, and investments in technology and skills. Key risks – legal,

political, and technical – must be mitigated through robust agreements (to guarantee immunity and jurisdiction), broad stakeholder buy-in, and sustainable funding strategies.

The recommendations chart a path whereby Sint Maarten's policymakers can create an enabling environment (via law reform and institution-building), partner with trusted allies for hosting and expertise, and implement the project in phases with proper safeguards. By doing so, Sint Maarten would join the ranks of innovators like Estonia in pioneering the concept of digital sovereignty through data embassies. The end result would be a stronger assurance that, come what may – be it hurricane, cyberattack, or other crisis – the essential records and services of the Sint Maarten government remain secure and accessible, thereby protecting its citizens and the continuity of the state. All steps should be documented and aligned with legal best practices, ensuring that this bold initiative stands on a firm footing of law, policy, and international cooperation.

6 Conclusion

