The impact of data legislation on regional data sharing: a Caribbean Legislation Review

An overview of Caribbean data legislation in the 15 CARICOM member states

Prepared by: Selvi Jeyaseelan, Ian Hambleton

Version 1: *October 2024*
Version 2: *June 2025*

Scope and Methods

In this review we focus on identifying and summarizing key legislation relevant to data handling across CARICOM member states. We have broadly interpreted "data handling" to include the creation, access, storage, transmission, and dissemination of data, particularly data of public health, administrative, or commercial relevance. We have placed special emphasis on how such laws might enable or restrict data sharing activities within and across national boundaries. We also focus particularly on data protection legislation, which we consider the main legal tool affecting data sharing.

Study Design

We conducted a structured policy and legislative review to examine the legal environment governing data handling across CARICOM member states. Our approach was designed to ensure transparency, reproducibility, and alignment with best practices for reporting non-interventional reviews, drawing on the PRISMA 2020 guidelines where applicable.

Objective

The primary objective of our review was to map the legal landscape of data governance in CARICOM countries, with particular attention to legislation affecting data producers—including government ministries, academic institutions, companies, and individuals. A secondary objective was to explore the implications of legal similarities and differences across countries for regional data sharing and integration.

PRISMA standards for review reporting

We have adopted the PRISMA standards for reporting this review. PRISMA provides structured reporting standards for various types of literature reviews. The PRISMA 2020 Statement includes a checklist of 27 items intended to ensure clarity, transparency, and reproducibility (1). While PRISMA is designed for systematic reviews, its principles are widely applicable to narrative reviews, scoping reviews, and legal or policy reviews, especially in areas like health governance and regulation.

We report key PRISMA 2020 items relevant to this review including:

- Item 5 (Eligibility Criteria): We have specified the inclusion and exclusion criteria for the review and how studies were grouped for the syntheses.
- Item 6 (Information Sources): We have listed all databases, registers, websites, organizations, reference lists, and other sources searched or consulted to identify studies.

- Item 7 (Search Strategy): We present our full search strategies used for our chosen databases, registers and websites, including any filters and limits used.

- Item 9 (Data Collection Process): We have specified the methods used to collect data from reports, including how many reviewers collected data, and whether they worked independently.

- Item 10b (Data Items): We have listed and defined all other variables for which data were sought (e.g., country name, year of law, legal category).

- Item 12 (Risk of Bias): Although not entirely applicable, for this legal reviews we have included discussion of completeness, currency, and source credibility.

- Item 20c (Results of Syntheses): We have described how the results of the review inform future policy or action.

Scope and Eligibility Criteria

We included legislation that:

- Originated from a full CARICOM member state

- Was officially enacted or in force as of May 2025 (we have noted one country—Suriname—that has drafted but not enacted Data Protection legislation)

- Addressed personal data protection, access to information, electronic transactions, or cybercrime

- We used legislation that was publicly available in English or through an official translation as our primary source. One country—Suriname—had no official translation for its draft legislation and we generated an unofficial English translation.

Except for Data Protection legislation (our primary focus), we excluded draft bills, unofficial summaries, or academic commentary unless these significantly impacted interpretation or current practice.

Country Selection

We targeted all 15 full CARICOM member states to ensure regional comprehensiveness. We reviewed each country individually. For countries participating in the IDB-funded CaribData project (Belize, Guyana, Jamaica, Trinidad and Tobago), we conducted a more in-depth assessment to support operational relevance.

For each country, the most recent national legislation relevant to data protection was identified and reviewed. Where no enacted Data Protection legislation existed, official draft bills (if publicly available) were reviewed in lieu of legislation. Legislation was sourced from government websites or official gazettes, and when necessary, unofficial English translations were generated (e.g., for Suriname).

Information Sources

To identify relevant legislation, we systematically consulted the following sources:

- Official government and parliamentary websites

- National legal portals and digital law repositories

- Government gazettes

- Regional and international databases (e.g., Caribbean Law Online, WIPO Lex, Lex Caribbean)

- Freedom of Information (FOI) portals, where available
- University law libraries and regional bar association databases
- Supplementary grey literature (such as policy briefs, academic publications).

The latest iteration of our searches were completed between March and May 2025.

Search Strategy

We used a standardized keyword strategy tailored to each CARICOM country. Keywords were:

"Data Protection Act", "Freedom of Information Act", "Electronic Transactions Act", "Computer Misuse Act", "Cybercrime Act", combined with the official name of each country.

The following 15 full CARICOM member states were included in the review: Antigua and Barbuda, The Bahamas, Barbados, Belize, Dominica, Grenada, Guyana, Haiti, Jamaica, Montserrat, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, Trinidad and Tobago.

Searches were conducted using Google / Google Scholar and internal search engines on national and regional legal portals. We applied no restrictions on publication year and (except for Data Protection legislation – our primary review focus) we limited inclusion to English-language texts or official translations. We supplemented keyword searches with manual reviews of legal indexes and gazette archives to identify uncatalogued or recently updated legislation.

Data Extraction and Management

We developed a structured data extraction form using Microsoft Excel. For each country, we extracted the following information for each law:

- Full title of the legislation
- Year of original enactment and most recent amendment (if applicable)
- Legal categorization framework (see below)
- Scope and key provisions
- Responsible enforcement agency
- Relevance to data sharing (and see our methods for creating our data protection heatmap)
- Notes on implementation or gaps (when available)

A single researcher (SJ) extracted data across all countries. A second reviewer (IH) independently checked 20% of entries to ensure consistency and completeness. Discrepancies were resolved through discussion.

Data synthesis: Categorization Framework

We grouped the laws into four major legal categories:

1. Data Protection: Laws that govern the collection, storage, use, and sharing of personal data, often emphasizing transparency, consent, and privacy.
2. Cybercrime / Computer Misuse: Legislation criminalizing unauthorized access, hacking, and digital infrastructure threats.

3. Freedom of Information (FOI): Laws that grant public access to government-held information, promoting transparency and accountability.

4. Electronic Transactions: Laws enabling the legal use of digital signatures, contracts, and communications in commerce and public service delivery.

When laws overlapped more than one category, we documented them under all relevant headings.

Thematic Synthesis

We performed a thematic synthesis for Data Protection legislation. This synthesis aimed to systematically compare the data protection legislation of each of the 15 CARICOM member states against nine features derived from the European Union General Data Protection Regulation (GDPR) (2), focusing specifically on how these features enable or restrict lawful and responsible data sharing.

Visualization of results: heatmap

We summarized our synthesis in a heatmap, with our nine GDPR features as rows, and Data Protection legislation from each CARICOM country represented as a column.

Selection of Comparator Framework

We selected the European Union's GDPR as the benchmark framework for comparison, given its comprehensive scope and its status as one of the most rigorous international standards in data protection. The GDPR explicitly addresses data sharing, consent, accountability, and individual rights in a way that supports cross-border data use, including for research and for public good.

Definition of GDPR-Based Features

We chose nine key features of the GDPR for their relevance to data producers seeking to share data responsibly. These were drawn directly from the GDPR's Articles and Recitals and are summarized as:

1. *Is there a clear legal reason to share data?*
   Looks at whether the law explains what makes data sharing lawful — like consent, public interest, or legal duties.

   GDPR Coverage: Article 6 outlines six lawful bases for processing, including consent, public interest, legal obligation, and legitimate interest.

2. *Does the law say who is responsible when data is shared?*
   Checks if the roles of data holders, users, and third parties are clearly defined, so everyone knows their duties.

   GDPR Coverage: Articles 4, 24–30 clearly distinguish roles of data controllers, processors, and joint controllers.

3. *Are the rules for getting consent clear and practical?*
   Assesses whether consent must be freely given, informed, and if the law says when consent is or isn't needed.

   GDPR Coverage: Articles 4(11) and 7, plus Recitals 32–43, define what valid consent looks like (freely given, informed, specific, unambiguous).

4. *Are people's rights protected when data is shared?*
   Ensures individuals can still access their data, ask for changes or deletion, and know who has their information.

GDPR Coverage: Articles 12–22 provide strong rights: access, correction, erasure, objection, restriction, and notification about data use — even when shared.

5. *Can data be shared safely if personal details are removed?*
   Looks at whether the law supports anonymizing or masking data to make sharing safer and easier.

   GDPR Coverage: Recital 26 states that anonymized data is not considered personal data and is not subject to GDPR. Articles 4 and 32 encourage pseudonymization as a safeguard when anonymization is not possible.

6. *Can data be shared with people or organizations in other countries?*
   Examines if there are clear rules for international data sharing, including when it's allowed and how.

   GDPR Coverage: Chapter V outlines strict rules for cross-border transfers, requiring adequacy decisions or safeguards like Standard Contractual Clauses (SCCs).

7. *Is there a public body that oversees data sharing and helps resolve problems?*
   Checks whether there's an independent authority to give guidance, monitor practices, and handle complaints.

   GDPR Coverage: Articles 51–59 require each EU member state to establish an independent supervisory authority with investigative and enforcement powers.

8. *Do data producers have to keep records and be open about sharing?*
   Looks at whether sharing activities must be documented and shared with regulators or data subjects.

   GDPR Coverage: Article 30 requires controllers/processors to document data flows, including sharing. Articles 13–14 require transparency with individuals about who their data is shared with.

9. *Does the law support data sharing for research and the public good?*
   Reviews whether sharing is allowed for scientific, health, or public interest purposes, with appropriate safeguards.

   GDPR Coverage: Articles 89 and Recitals 157–163 allow processing and sharing for scientific research, statistics, and public health, with safeguards. Member states may add specific rules to facilitate this.

Each of these features is well-defined in the GDPR and was used as a fixed reference point for comparing national laws.

Scoring Process

We assessed each country's legislation against the nine GDPR features using a five-level scoring system that reflected the degree of alignment:

Score	Category Alignment	Heatmap Color	Category Interpretation
5	Excellent alignment	Deep Green	Closely mirrors GDPR with minimal deviation
4	Good alignment	Light Green	Substantially similar to GDPR with minor gaps
3	Moderate alignment	Yellow	Partial coverage with room for clarification
2	Poor alignment	Orange-Red	Limited coverage or clarity
1	Very poor alignment	Deep Red	No alignment or highly restrictive/conflicting

Our assessment was conducted by reviewing each law and mapping its clauses, articles, and definitions against the corresponding GDPR provisions. Emphasis was placed on functional equivalence rather than word-for-word alignment. For example, we did not penalize legislation for lacking implementation details, provided it clearly enabled the GDPR-equivalent feature.

Review and Documentation

We justified the legislation alignment with GDPR features in plain English using short explanations, which we included in our heatmap. We wrote these justifications to be understandable to a general audience, with technical or legal jargon avoided where possible. Each cell displayed the color-coded score along with the corresponding justification.

To maintain transparency and reproducibility the GDPR full text and each national Act or draft Bill were retained as source documents.

Summary Scoring

An informal summary score for each country and for each GDPR feature was calculated by converting each cell's score to a numerical value and summing across the nine features. This enabled the creation of an informal overall ranking of countries by GDPR alignment.

Limitations and Bias Considerations

While we aimed for completeness, legislation was sometimes unavailable in digital form, or only accessible through secondary commentary. Some national repositories were incomplete or outdated. We relied on English sources, which may have limited our access to recent amendments in countries where legislative documents were not translated or publicly released. Although we did not formally assess risk of bias, we considered credibility of source, publication date, and official status in our inclusion decisions.

Results: Regional overview

Legislative Trends in CARICOM Data Governance

The types of Acts enacted in each country, along with their year of enactment are presented in Table 1.

Table 1: Summary comparison of enacted common data related legislation among CARICOM member states

Country	Data Protection	Computer Misuse	Electronic Transactions	Freedom of Information
Antigua & Barbuda	2013	2020	2016	2004
The Bahamas	2003	2003	2003	2017
Barbados	2019	2005	2014	Draft (2008)
Belize	2021	2020	2003	2011
Dominica	-	-	2013	-
Grenada	2023	2013	2013	-
Guyana	2023	2018	2023	2011
Haiti	-	-	-	-
Jamaica	2020	2015	2006	2002
Montserrat	-	2022	-	-
St Kitts & Nevis	2018	2017	2011	2024
St Lucia	2011	2011	2014	-
St Vincent & Grenadines	2003	2016	2015	2003
Suriname §	-	-	-	-
Trinidad & Tobago	2016	2016	2016	2016

§ Suriname Privacy and Personal Data Protection Law (2020) has been drafted, and is not yet active

The adoption of data-related legislation across CARICOM countries reveals a staggered but growing commitment to digital governance. A key observation relates to Data Protection Acts, which have gained significant traction post-2018, after the implementation of the EU General Data Protection Regulation (GDPR). Notably, six out of the eleven CARICOM countries with enacted data protection laws passed them since 2018—St Kitts and Nevis (2018), Barbados (2019), Jamaica (2020), Belize (2021), Guyana (2023), and Grenada (2023)—suggesting strong influence from the GDPR model and its emphasis on privacy, consent, and accountability. Earlier adopters like The Bahamas (2003) and St Lucia (2011) reflect pre-GDPR frameworks that may now be considered in need of modernization to align with international standards.

For Computer Misuse legislation, adoption began as early as 2003 (Bahamas), but gained momentum post-2015. These laws address the rising threat of cybercrime, with most nations enacting statutes between 2015 and 2022. This mirrors global trends following increased awareness of cyber threats and the 2013–2017 uptick in ransomware and government breaches worldwide. The Budapest Convention on Cybercrime, while not ratified by most CARICOM nations, appears to have indirectly influenced these laws (3).

Electronic Transactions laws were among the earliest digital laws adopted in the region, reflecting a focus on enabling e-commerce and digital government. Eleven countries have enacted such laws, with early movers like The Bahamas and Belize in 2003, and more

recent adoption by Guyana in 2023. This suggests growing prioritization of digital trade and service delivery across the region.

Finally, Freedom of Information (FOI) legislation is the most inconsistently adopted framework. Only eight countries have enacted FOI laws, with significant delays or absences in others. The earliest adopters—Jamaica (2002) and Antigua & Barbuda (2004)—contrast with newer efforts in St Kitts & Nevis (2024) and The Bahamas (2017). The patchy implementation reflects challenges in transparency culture, administrative capacity, and political will, a pattern noted in global assessments of FOI law effectiveness in small states.

Overall, CARICOM countries are progressively building their digital governance infrastructure. The GDPR appears to have acted as a catalytic force for modern data protection regimes, while regional responses to cyber threats and e-commerce imperatives are shaping broader digital legal frameworks. However, freedom of information remains an unevenly addressed pillar, underscoring ongoing barriers to open governance.

Data Protection Legislation: alignment with GDPR data sharing features

Our synthesis of data protection legislation with comparison against the 9 data-sharing features of GDPR is presented in Figure 1. This heatmap summarizes the extent to which national data protection laws across 15 CARICOM full member states align with nine core GDPR features specifically related to enabling lawful and safe data sharing.

General Patterns of Alignment

CARICOM countries show wide variation in how closely their laws align with GDPR principles. While no country achieves full GDPR alignment, a small number—particularly those that have enacted or revised legislation in the post-GDPR era—come close in several areas. Notably, Barbados, Belize, Suriname, and Trinidad & Tobago demonstrate relatively strong alignment, with legislation that includes most of the GDPR-informed features needed to support lawful, rights-based data sharing.

These newer laws incorporate detailed provisions on consent, data subject rights, and in some cases, mechanisms for safe sharing through pseudonymisation or specified public interest exceptions. This suggests growing convergence with international norms and offers a strong foundation for further refinement.

In contrast, several countries with older or less developed legislation—such as Dominica and Grenada—lack key safeguards, resulting in major gaps that limit their ability to safely and ethically share personal data, even for socially valuable purposes such as research or public health.

Common Strengths Across the Region

Two GDPR-aligned features are reflected more consistently across the region:

1. *Legal Bases for Data Sharing*
   Most countries legally permit data sharing under certain conditions, such as when individuals consent, when the law requires it, or for the public good. For example, Suriname and Trinidad & Tobago clearly list lawful grounds for data use and sharing, closely tracking the structure of GDPR Article 6. This alignment is a critical enabler of responsible data use across sectors.

2. *Rights of Data Subjects*
   A growing number of countries—including Barbados, Belize, and St. Kitts and Nevis—grant individuals the right to access, correct, or delete their data. These provisions reflect GDPR principles of transparency and control and are vital for building trust in digital systems.

Ongoing Gaps and Challenges

Despite this progress, significant gaps remain in three key areas necessary for safe and effective data sharing:

1. *Data Safeguards Like Anonymisation*
   Most CARICOM data protection laws either omit or only briefly mention techniques like anonymisation and pseudonymisation. These are critical tools under GDPR for reducing risk when data is shared, particularly in health, education, and research.

2. *Defined Roles and Responsibilities*
   Some laws do not clearly define the responsibilities of entities that collect and use data (data controllers) versus those that process data on their behalf (data processors). This can create confusion over who is accountable for protecting personal data, especially when multiple organisations are involved in data sharing.

3. *Oversight and Enforcement*
   Few countries have established fully independent data protection authorities with the legal power to oversee data sharing and enforce compliance. The lack of such institutions limits individuals' ability to seek redress and undermines confidence in data governance systems.

Position Relative to Global Trends

The review highlights that CARICOM's most recently enacted laws are beginning to reflect the growing global shift toward strong, interoperable data governance. For instance:

- The OECD's 2022 Declaration on Government Access to Personal Data and initiatives like the Global Cross-Border Privacy Rules Forum promote secure international data flows through clearly defined rights and safeguards.

- The WHO Health Data Governance Framework (2021) emphasises ethical reuse of data based on transparency, consent, and protective technical measures—principles that are gradually appearing in Caribbean legislation.

Nonetheless, the lack of consistency across CARICOM presents risks. Without coordinated progress, the region may struggle to participate fully in cross-border research, digital public services, and data-driven trade opportunities.

Opportunities for Regional Action

CARICOM has the opportunity to build on the strong foundations laid by its newer legislation. Regional priorities should include:

- Developing common standards for data anonymisation and secure sharing, adapted for Caribbean contexts.

- Clarifying responsibilities across the data lifecycle to improve accountability.

- Investing in independent oversight bodies with the mandate and capacity to enforce laws and protect citizens' rights.

- Pursuing legislative harmonisation to support regional interoperability and foster public and private sector data use.

Further Analysis: Legal Nuances in Data Protection Across CARICOM

Building on the earlier comparison of legislation types, we undertook a more granular examination of data protection frameworks across CARICOM member states. While all four types of digital legislation—Data Protection, Computer Misuse, Electronic Transactions, and Freedom of Information—shape the information landscape, data protection laws are the most consequential for enabling or constraining data sharing, particularly in health, research, and public sector transformation.

These laws define the rules for collecting, processing, and transferring personal data, and their strength directly affects the region's capacity to participate in trusted, rights-based data flows. Globally, there is increasing recognition—from the OECD, WHO, and G7 Data Free Flow with Trust (DFFT) initiatives—that data sharing is a cornerstone of digital development, but must be grounded in ethical, secure, and interoperable systems.

Shared Foundations: A Move Toward Common Principles

Despite differences in national contexts, CARICOM data protection laws show a promising degree of alignment with international norms, reflecting the influence of the EU's General Data Protection Regulation (GDPR) and other global instruments.

Common strengths include:

- Core data protection principles (e.g., purpose limitation, accuracy, data minimisation, fairness) are found across most CARICOM country laws.
- Independent oversight bodies such as Data Protection Authorities or Commissioners have been broadly established to ensure legal compliance, transparency, and redress.
- Explicit consent is generally required for processing sensitive personal data, echoing global concerns over dignity, privacy, and non-discrimination.
- Public interest exemptions—national security, journalism, legal proceedings—reflect a balance between protection and freedom of expression, a theme in the UN's Global Digital Compact (4).

This convergence suggests that CARICOM countries are increasingly participating in the global policy turn toward accountable and enabling data environments.

Divergences That Matter: Legal Scope and Enforcement

Despite these shared foundations, implementation details diverge significantly, affecting not only national effectiveness but also regional interoperability—a key challenge identified in global data cooperation efforts.

Key Areas of Difference:

- Scope of Application
  Some countries (such as Barbados, Jamaica, Trinidad & Tobago) extend protections extraterritorially, covering foreign entities processing citizen data. This aligns with global best practices and the Council of Europe's Convention 108+ (5). However, a minority of CARICOM country laws remain focused only on domestic entities.
- Registration Requirements
  Mandatory registration and penalties in (for example) Barbados, Guyana, and Jamaica help formalize data governance ecosystems. In contrast, Grenada and St Kitts & Nevis adopt lighter-touch approaches, which may reduce

administrative burden but complicate enforcement and coordination.

- Privacy Impact Assessments (PIAs)
  Required in for example Jamaica, St Lucia, and Trinidad & Tobago, PIAs reflect increasing global emphasis on risk-based regulation—a core recommendation in OECD's 2022 Declaration on Government Access to Personal Data (6).

- Enforcement Mechanisms
  Fines vary from stringent (e.g., Barbados: BBD $500,000) to symbolic (e.g., St Lucia: lesser penalties), affecting both deterrence and perceived legitimacy of regulatory frameworks.

Data Sharing in Practice: National and Cross-Border Perspectives

Within-Country Data Sharing

Internationally, data stewardship is emerging as a framework that supports responsible reuse of data for public good—particularly in health, climate, and education. CARICOM country laws show early movement in this direction:

- The Jamaican data protection Act lays out plans to issue a Data Sharing Code, aligning with OECD and UK practices in transparent guidance for public authorities.
- Trinidad & Tobago requires Commissioner approval for inter-agency data sharing, reducing unchecked data flows.
- Belize allows structured agreements that mirror evolving models of data trusts and data collaboratives elsewhere in the Global South (7).

These mechanisms signal a regional shift toward formal, transparent agreements that help build trust and clarify responsibilities.

Cross-Border Data Sharing

The ability to transfer data across borders—securely and ethically—is a key enabler of participation in the global digital economy. While almost all CARICOM countries formally enable transfers under certain safeguards, the absence of harmonised standards risks fragmentation.

Global Parallel—Initiatives like the Global Cross-Border Privacy Rules (CBPR) Forum, Africa's Policy Framework on Cross-Border Data Flows, and Latin America's REDIPD have shown that regional coordination is crucial for enabling trusted, scalable data exchanges (8).

CARICOM could follow suit by:

- Developing a regional adequacy framework for mutual recognition.
- Aligning national safeguards with international interoperability models.

Examples from the Region:

- Barbados and Belize permit binding corporate rules and Commissioner-led oversight for outbound transfers.
- Trinidad & Tobago mandates prior assessment of receiving countries or explicit consent with defined limits.

Summary and Global Relevance

CARICOM's evolving data protection frameworks reflect strong foundational alignment and growing ambition to participate in trusted international data ecosystems. While

internal legal divergences and limited enforcement capacity pose barriers, global momentum offers models for reform.

Incorporating global themes such as:

- Interoperability over harmonisation,
- Data stewardship for public good, and
- Cross-border trust frameworks,

can help CARICOM countries move from policy alignment to practical collaboration—especially in areas like regional health surveillance, digital trade, and climate resilience.

Discussion and Conclusion

This review reveals that while CARICOM countries have made notable legislative progress in regulating digital environments, particularly around personal data protection, the region remains at a crossroads. Emerging global movements underscore that robust, interoperable data governance is no longer optional—it is essential for development, trust, and digital sovereignty. The Caribbean must move from static legal frameworks to dynamic, enabling ecosystems where rights, responsibilities, and regional collaboration coexist.

From Legal Foundations to Functional Systems

The analysis illustrates a growing legislative maturity across CARICOM, particularly in data protection. Several countries—most notably Barbados, Belize, Grenada and Jamaica—have enacted laws with strong conceptual alignment to international norms, such as the EU General Data Protection Regulation (GDPR). These frameworks reflect a deepening regional understanding of data as both a protected asset and a strategic resource.

However, legislative adoption is uneven, and implementation remains a significant challenge. Several countries still lack data protection laws entirely. Others have enacted laws without bringing them fully into force or resourcing their enforcement bodies. This legal fragmentation undermines the potential for effective data sharing, both within countries and across borders.

Emerging Global Trends in Data Sharing: Lessons for CARICOM

Across the world, data governance is evolving beyond binary debates over openness vs. privacy, toward frameworks that support responsible data reuse in the public interest. Several global initiatives are particularly instructive for the Caribbean context:

- OECD's 2023 Framework for Data Ecosystems promotes "data action frameworks" that integrate governance, institutions, and capability development. It argues for policies that enable cross-sectoral and cross-border data use, grounded in transparency, accountability, and shared value creation (9).

- The African Union's 2022 Data Policy **Framework** encourages member states to align on regional principles for data sovereignty, interoperability, and infrastructure—while recognizing national diversity. It supports legal harmonization and common data sharing protocols to enable a digital single market (10).

- India's Digital Public Infrastructure model, built on open standards and modular regulation, shows how legal frameworks, consent management, and public oversight can co-evolve with digital services. India's Data Empowerment and Protection Architecture (DEPA) enables safe, granular data sharing in sectors like finance and health, using user-controlled consent layers.

- The Latin American REDIPD (Red Iberoamericana de Protección de Datos) fosters cross-border data protection dialogue, coordinated enforcement, and shared evaluation metrics across jurisdictions with diverse legal systems—offering a peer-driven alternative to top-down harmonization.

- The Global Partnership on AI (GPAI) and UNESCO's Recommendation on the Ethics of AI (2021) both highlight the need for legal environments that allow data to be reused responsibly for innovation and public good, while ensuring inclusivity and ethical safeguards—principles that are vital for Caribbean small states with limited data capacity (11).

A Caribbean Imperative: From Alignment to Action

The Caribbean has a unique opportunity to design data governance that reflects its regional values—equity, cooperation, public good—and advances collective development goals. Doing so requires moving beyond legislative alignment to action across four strategic areas:

1. Regulatory Operationalization
   Legislation must be activated through regulations, guidance, institutional mandates, and public awareness. A law without enforcement mechanisms or public legitimacy can create more uncertainty than clarity. For instance, while several countries now have Data Commissioners on paper, few have full investigatory and redress functions in practice.

2. Harmonization Through Mutual Recognition
   While full legal harmonization may be politically or constitutionally difficult, mutual recognition agreements—where countries acknowledge each other's data safeguards as "adequate"—could provide a practical path toward trusted regional data flows.

3. Data Stewardship and Sectoral Protocols
   Countries like the UK and South Africa have pioneered sector-specific data sharing codes (e.g. in health, education, or social care) that provide detailed operational guidance. CARICOM countries could similarly adopt shared protocols in health, disaster response, or climate surveillance—areas of urgent collective concern.

4. Investment in Capability and Culture
   As the OECD and UNDP both emphasize, data governance requires more than laws—it needs people, tools, and trust. Caribbean governments should invest in technical training, public engagement, and institutional capacity to ensure that data protection is a catalyst for responsible use rather than a legal constraint.

Conclusion: A Pathway to Trusted Regional Data Ecosystems

This review demonstrates that CARICOM is on the threshold of building a regionally coherent and internationally credible data governance architecture. The legislative foundations are largely in place. But to unlock the transformative potential of data—in research, public services, economic development, and climate resilience—the region must focus on integration, implementation, and innovation.

CARICOM should consider a roadmap for a Trusted Regional Data Ecosystem, built on five pillars:

- Common legal standards rooted in shared principles but adaptable to national context

- Mutual trust mechanisms to support lawful cross-border data flows

- Independent and capable regulators that build public confidence
- Data stewardship models that balance protection with societal reuse
- Participatory governance involving civil society, academia, and the private sector

Such a model would not only align the region with global best practices but would also assert a Caribbean voice in global digital governance debates—where small states have much at stake and much to offer.

References

1. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ. 2021 Mar 29;n71.

2. European Commission. Directorate General for Justice and Consumers. The GDPR: new opportunities, new obligations : what every business needs to know about the EU's General Data Protection Regulation. [Internet]. LU: Publications Office; 2018 [cited 2025 Jun 29]. Available from: https://data.europa.eu/doi/10.2838/97649

3. Wicki-Birchler D. The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? Int Cybersecurity Law Rev. 2020 Oct;1(1–2):63–72.

4. Wylde A. The UN Global Digital Compact (GDC), Achieving a trusted, free, open, and Secure Internet: Trust-building. Eur Conf Cyber Warf Secur. 2023 Jun 19;22(1):544–51.

5. De Terwangne C. Council of Europe convention 108+: A modernised international treaty for the protection of personal data. Comput Law Secur Rev. 2021 Apr;40:105497.

6. Docksey C, Propp K. Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective. Oslo Law Rev. 2023 Nov 14;10(1):1–34.

7. GPAI. Trustworthy Data Institutional Framework: A practical tool to improve trustworthiness in data ecosystems, [Internet]. Global Partnership on AI; 2023 [cited 2025 Jun 29]. Available from: https://gpai.ai/projects/data-governance/data-trusts/

8. Callo-Müller MV. From APEC to Global: The Establishment of the Global CBPR Forum. Glob Trade Cust J. 2025 Feb 1;20(Issue 2):130–43.

9. 2023 OECD Open, Useful and Re-usable data (OURdata) Index: Results and Key Findings [Internet]. 2023 Dec [cited 2025 Jun 29]. (OECD Public Governance Policy Papers; vol. 43). Report No.: 43. Available from: https://www.oecd.org/en/publications/2023-oecd-open-useful-and-re-usable-data-ourdata-index_a37f51c3-en.html

10. African Union Commission, Department of Infrastructure & Energy. AU Data Policy Framework [Policy framework] [Internet]. Endorsed by Exec. Council Decision EX.CL/Dec.1144(XL), 2–3 Feb 2022.; 2022 Jul [cited 2025 Jun 29]. Available from: https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf?utm_source=chatgpt.com

11. The UNESCO recommendation on the Ethics of AI: shaping the future of our societies. Status April 2023. Bonn, Den Haag, Ljubjana: German Commission for UNESCO e.V. Netherlands National Commission for UNESCO Slovenian National Commission for UNSESCO; 2023.

Appendices

AG Antigua and Barbuda: Data Legislation Snapshot

1. Data Protection Act, 2013
Purpose: Safeguards personal data across public/private sectors.
Scope: All data processed in commercial or official contexts.
Key Points:

- Data must be processed lawfully and securely, with consent where required.
- Emphasizes accuracy, retention limits, and data subject rights.
- Exemptions: law enforcement, journalism, research, public interest.

For Data Producers: Follow core data principles; violations can lead to fines or jail. Oversight by Information Commissioner.

2. Electronic Crimes Act (Amended), 2020
Purpose: Expands investigatory powers and adds offences.
Scope: Covers cybercrimes including money laundering and customs.
Key Points:

- Grants data access powers to ONDCP and Customs, not just police.
- Includes real-time traffic data and broader seizure authority.

For Data Producers: May need to support investigations with data access or compliance during cybercrime probes.

3. Electronic Transactions Act, 2016
Purpose: Clarifies gov't obligations around electronic records.
Scope: Digital communications with ministries/public bodies.
Key Points:

- Gov't not required to process electronic records unless stated.
- Ministries can set own rules for format, e-signatures, and security.

For Data Producers: Must meet tech requirements if submitting to government electronically.

4. Freedom of Information Act, 2004
Purpose: Enhances public access to government-held info.
Scope: Applies to all public bodies.
Key Points:

- Individuals can request access to public information.
- Bodies must proactively publish key documents and assign Info Officers.

For Data Producers: Ensure proper record keeping and timely responses; annual FOI reports mandatory.

BS Bahamas: Data Legislation Snapshot

1. Data Protection (Privacy of Personal Information) Act, 2003
Purpose: Protects individual privacy and regulates data use.
Scope: Applies to entities handling personal data in or through The Bahamas.
Key Points:
• Establishes rights: access, correction, erasure of personal data.
• Creates a Data Protection Commissioner.
• Restricts international data transfers without safeguards.
For Data Producers: Ensure lawful, fair, and secure data processing. Be prepared for audits and enforceable access rights.

2. Computer Misuse Act, 2003
Purpose: Criminalizes unauthorized access and computer misuse.
Scope: Applies within and outside The Bahamas accessing local systems.
Key Points:
• Covers unauthorized access, system damage, and code misuse.
• Enhanced penalties for critical infrastructure attacks.
For Data Producers: Protect against unauthorized access and assist law enforcement when required.

3. Electronic Communications and Transactions Act, 2003
Purpose: Grants legal recognition to electronic records and transactions.
Scope: Applies to digital contracts, signatures, and communications.
Key Points:
• Digital records/signatures have legal equivalency.
• E-commerce providers have defined liability and content rules.
For Data Producers: Ensure digital record integrity and meet e-commerce compliance standards.

4. Freedom of Information Act, 2017
Purpose: Facilitates access to public sector information.
Scope: Applies to designated public authorities.
Key Points:
• Grants access rights to government-held records.
• Supports appeals and oversight by Information Commissioner.
For Data Producers: Maintain searchable records, train staff, and implement access procedures.

BB Barbados: Data Legislation Snapshot

1. Data Protection Act, 2019
Purpose: Safeguards personal data and promotes privacy rights.
Scope: Applies to any entity processing data of Barbadian residents.
Key Points:
• Requires fair processing, consent, and transparency.
• Mandates registration and breach notification.
• Covers sensitive data, children, and automated profiling.
For Data Producers: Register with Commissioner, uphold consent, and implement secure, rights-based processing systems.

2. Computer Misuse Act, 2005 / Cybercrime Bill (Draft, 2024)
Purpose: Addresses cyber threats and unauthorized system access.
Scope: Applies locally and abroad if harm is within Barbados.
Key Points:
• Covers hacking, interception, data interference, and child exploitation.
• Draft bill expands to cyberbullying and terrorism.
For Data Producers: Enforce strong cybersecurity and assist law enforcement. Prepare for future requirements if the bill passes.

3. Electronic Transactions (Amendment) Act, 2014
Purpose: Strengthens e-commerce and digital communication framework.
Scope: Covers electronic trade, certification services, and digital identity.
Key Points:
• Defines certified signatures and provider licensing.
• Includes consumer protections and dispute rules.
For Data Producers: Ensure licensing, transparency, and reliable records when offering digital services.

4. Freedom of Information Bill (Draft, 2008)
Purpose: Grants constitutional access to public records.
Scope: Covers most public authorities, excluding judiciary and parliament.
Key Points:
• Proposes Info Commissioner and public information roles.
• Allows request refusals based on clear exemptions.
For Data Producers: Prepare records systems and policies for future FOI requests if enacted.

BB Belize: Data Legislation Snapshot

1. Data Protection Act, 2021
Purpose: Regulates data processing and protects privacy rights.
Scope: Applies to public and private actors targeting Belize residents.
Key Points:
• Defines subject rights, cross-border rules, and breach duties.
• Creates Data Protection Commissioner and Tribunal.
For Data Producers: Ensure consent, assess privacy impacts, and report breaches. Prepare for enforcement actions.

2. Cybercrime Act, 2020
Purpose: Penalizes cyber offences and ensures investigatory powers.
Scope: Applies to local and international digital threats impacting Belize.
Key Points:
• Covers hacking, identity theft, stalking, and fraud.
• Enables search, preservation, and cross-border cooperation.
For Data Producers: Apply strong security and retain logs when requested. Comply with investigative demands.

3. Electronic Transactions Act, 2003
Purpose: Removes barriers to digital commerce and official e-documents.
Scope: Covers most digital transactions except land and wills.
Key Points:
• Grants legal status to e-documents and signatures.
• Outlines consent, format, and data retention standards.
For Data Producers: Adopt valid e-signatures and storage standards. Align with public body expectations.

4. Freedom of Information Act, 1994
Purpose: Enables public access to government information.
Scope: Applies to all public authorities in Belize.
Key Points:
• Allows document access unless exempted (e.g., security).
• Sets response timelines and appeal rights.
For Data Producers: Catalog and manage records for FOI readiness. Apply exemption logic when needed.

BB Dominica: Data Legislation Snapshot

1. Data Protection
Purpose: No dedicated law; governed by constitutional rights.
Scope: Applies to privacy, expression, and public data under the Constitution.
Key Points:
• No explicit data protection legislation.
• Public data use must respect individual rights.
For Data Producers: Ensure all public data work aligns with constitutional privacy and access guarantees.

2. Electronic Crimes / Cybercrime
Purpose: No cybercrime law currently enacted.
Scope: No formal framework for computer misuse.
Key Points:
• Legal vacuum for cyber threats and hacking offences.
• Risks exist due to lack of enforcement provisions.
For Data Producers: Adopt internal cybersecurity best practices proactively.

3. Electronic Transactions Act, 2013
Purpose: Legalizes e-documents and contracts.
Scope: Covers individuals, businesses, and government (excludes land, wills).
Key Points:
• Gives e-records the same status as physical ones.
• Enables e-filing and e-commerce trust.
For Data Producers: Maintain secure digital records and compliant signature practices.

4. Freedom of Information
Purpose: No FOI law enacted.
Scope: FOI provisions not yet formalized.
Key Points:
• No legal right to public information access.
• Reduces transparency for government-held data.
For Data Producers: Support open data principles voluntarily where possible.

BB Grenada: Data Legislation Snapshot

1. Data Protection Act, 2023
Purpose: Protects personal data and establishes oversight.
Scope: Applies to all entities processing personal data in Grenada.
Key Points:
• Mandates consent and secure processing.
• Creates Information Commission with strong powers.
• Covers retention and rectification rights.
For Data Producers: Obtain consent and comply with subject rights. Expect audits and penalties for breaches.

2. Electronic Crimes Act, 2013
Purpose: Defines and punishes electronic crimes.
Scope: Covers local and foreign digital crimes affecting Grenada.
Key Points:
• Criminalizes hacking, fraud, identity theft, and encryption misuse.
• Authorizes real-time data seizure and law enforcement access.
For Data Producers: Implement strong security. Cooperate with legal requests for data.

3. Electronic Transactions Act, 2013
Purpose: Provides legal recognition for e-communications.
Scope: Covers e-contracts, signatures, and records (some exclusions).
Key Points:
• Ensures e-records are legally admissible.
• Includes consumer protection and intermediary rules.
For Data Producers: Use reliable e-systems and provide clear user information.

4. Freedom of Information
Purpose: No FOI legislation identified.
Scope: Transparency not formally legislated.
Key Points:
• Lack of public access law limits accountability.
• Calls for reform and openness remain ongoing.
For Data Producers: Apply good recordkeeping and voluntary transparency practices.

BB Guyana: Data Legislation Snapshot

1. Data Protection Act, 2023
Purpose: Regulates data handling and subject rights.
Scope: Applies to both public and private data controllers.
Key Points:
• Requires lawful, secure, and transparent processing.
• Subjects have access, correction, and erasure rights.
• Enforced by a dedicated commission.
For Data Producers: Audit systems for compliance. Respect rights and report breaches.

2. Cybercrime Act, 2018
Purpose: Criminalizes cyber threats and system abuse.
Scope: Covers broad offenses including cyberbullying and data theft.
Key Points:
• Addresses hacking, fraud, child abuse, identity crimes.
• Supports search, seizure, and international cooperation.
For Data Producers: Deploy cybersecurity frameworks and train staff. Data misuse can be criminally liable.

3. Electronic Communications and Transactions Act, 2023
Purpose: Facilitates secure digital transactions and communications.
Scope: Applies to e-services, commerce, and authentication.
Key Points:
• Recognizes e-documents and digital signatures.
• Defines provider liability and data integrity standards.
For Data Producers: Ensure reliable digital tools and traceable interactions. Store records securely.

4. Access to Information Act, 2011
Purpose: Grants citizens access to government information.
Scope: Applies to all public authorities except exempt bodies.
Key Points:
• Mandates publication and request procedures.
• Sets up a Commissioner for oversight.
For Data Producers: Build searchable archives and respond to requests promptly.

JM Jamaica: Data Legislation Snapshot

1. Data Protection Act, 2020
Purpose: Protects individual privacy and governs personal data processing.
Scope: Applies to data processors and controllers in or serving Jamaica.
Key Points:
• Grants data subjects access and correction rights.
• Requires consent, security, and breach notification.
• Creates the Office of the Information Commissioner.
For Data Producers: Comply with data standards, manage consent, and facilitate subject rights under a 2-year transitional period.

2. Cybercrimes Act, 2015
Purpose: Addresses a broad range of digital offences.
Scope: Applies to all entities involved in data misuse in Jamaica.
Key Points:
• Covers unauthorized access, modification, and harassment.
• Protects infrastructure and provides for strong penalties.
For Data Producers: Maintain secure systems and cooperate with cyber investigations and data preservation requirements.

3. Electronic Transactions Act, 2006
Purpose: Facilitates digital contracts and e-commerce.
Scope: Applies to most electronic transactions, with some exceptions.
Key Points:
• Recognizes e-documents and signatures as legally valid.
• Sets time/place of receipt rules and outlines certification responsibilities.
For Data Producers: Ensure e-documents are accurate, retrievable, and signed using accepted standards.

4. Access to Information Act, 2002
Purpose: Establishes public rights to government-held data.
Scope: Covers ministries, statutory bodies, and state-owned entities.
Key Points:
• Outlines request, refusal, and appeal processes.
• Includes security and privacy exemptions.
For Data Producers: Enable public access to official documents and handle requests in compliance with the Act.

KN Saint Kitts and Nevis: Data Legislation Snapshot

1. Data Protection Act, 2018
Purpose: Regulates personal data handling in commercial contexts.
Scope: Applies to public and private bodies involved in data processing.
Key Points:
• Requires consent, security, and limits on retention.
• Enforces access and correction rights through the Commissioner.
For Data Producers: Secure systems, manage consent, and comply with audits or enforcement.

2. Electronic Crimes Act (Revised), 2017
Purpose: Criminalizes digital misconduct.
Scope: Applies to cyber offences locally and abroad.
Key Points:
• Covers hacking, fraud, identity theft, and cyber espionage.
• Allows for remote forensics and data seizure.
For Data Producers: Safeguard systems and cooperate with investigations upon request.

3. Electronic Transactions Act, 2011
Purpose: Recognizes digital contracts and communications.
Scope: Applies to government and commercial e-records.
Key Points:
• Validates digital signatures and certified communications.
• Protects intermediary service providers.
For Data Producers: Maintain authentic, retrievable records and support e-signature infrastructure.

4. Freedom of Information (Amendment) Act, 2024
Purpose: Enhances the oversight and administration of FOI.
Scope: Applies to all public bodies under the FOI Act.
Key Points:
• Introduces Ombudsman and Special Prosecutor roles.
• Streamlines appointments and clarifies oversight.
For Data Producers: Ensure records are FOI-compliant and staff are trained on new procedures.

LC Saint Lucia: Data Legislation Snapshot

1. Data Protection Act, 2011 (Amended 2015)
Purpose: Safeguards personal data and privacy rights.
Scope: Applies to all controllers using equipment in Saint Lucia.
Key Points:
• Defines rights, duties, and data handling principles.
• 2015 amendment requires impact assessments and enhances enforcement.
For Data Producers: Register with the Commissioner, perform PIAs, and secure personal data across systems.

2. Computer Misuse Act, 2011
Purpose: Criminalizes cyber offences and system misuse.
Scope: Covers acts within and impacting Saint Lucia.
Key Points:
• Addresses hacking, interception, and access breaches.
• Allows search, seizure, and cooperation with police.
For Data Producers: Apply access controls, monitor compliance, and decrypt when legally required.

3. Electronic Transactions Act, 2011 (Amended 2014)
Purpose: Enables secure digital records and communications.
Scope: Covers local and cross-border e-transactions.
Key Points:
• Legalizes digital records and signatures.
• 2014 amendment allows staggered activation of provisions.
For Data Producers: Ensure technical compliance, monitor activation notices, and enable phased implementation.

4. Freedom of Information
Purpose: No dedicated FOI legislation yet.
Scope: Public access to data not formally guaranteed.
Key Points:
• FOI not enacted in law.
• Reduces accountability in public data access.
For Data Producers: Support open data informally until FOI legislation is passed.

VC Saint Vincent and the Grenadines: Data Legislation Snapshot

1. Privacy Act, 2003
Purpose: Protects individual privacy in public data systems.
Scope: Applies to personal data held by public authorities.
Key Points:
• Ensures access and correction rights.
• Creates Privacy Commissioner for oversight.
For Data Producers: Protect data integrity and grant correction access. Retain and dispose of data lawfully.

2. Cybercrime Bill, 2016
Purpose: Defines cyber offences and sets enforcement mechanisms.
Scope: Covers unauthorized access, fraud, and child abuse content.
Key Points:
• Criminalizes hacking, interference, and abuse online.
• Mandates ISP cooperation with removal and seizure.
For Data Producers: Comply with data preservation and takedown orders. Secure systems proactively.

3. Electronic Transactions Act, 2015
Purpose: Grants legal status to digital records and contracts.
Scope: Covers most digital business and government interactions.
Key Points:
• Recognizes e-documents and signatures.
• Supports international alignment and trust in e-commerce.
For Data Producers: Secure and manage e-records legally and transparently. Apply consumer safeguards.

4. Freedom of Information Act, 2003
Purpose: Enables public access to official records.
Scope: Applies to all public authorities with some exclusions.
Key Points:
• Grants request rights with exemptions (e.g. national security).
• Mandates record indexing and transparency.
For Data Producers: Support FOI readiness with structured systems and clear exemption logic.

TT Trinidad and Tobago: Data Legislation Snapshot

1. Data Protection Act, 2011 (Revised 2016)
Purpose: Regulates personal information processing and access rights.
Scope: Applies to public and private data users.
Key Points:
• Outlines 12 data privacy principles.
• Expanded scope includes audits, mediation, and codes of conduct.
For Data Producers: Implement data policies and cooperate with audits. Ensure cross-border and sensitive data controls.

2. Computer Misuse Act, 2000 (Revised 2016)
Purpose: Criminalizes digital interference and misuse.
Scope: Applies to misuse affecting or originating from T&T systems.
Key Points:
• Includes hacking, password leaks, and sabotage.
• Protects critical systems and defines police powers.
For Data Producers: Classify sensitive infrastructure and prepare logs. Provide audit trails during investigations.

3. Electronic Transactions Act, 2011 (Revised 2016)
Purpose: Supports secure digital trade and communications.
Scope: Applies to most public and private e-services.
Key Points:
• Legalizes e-documents, contracts, and authentication.
• Mandates transparency, traceability, and retention.
For Data Producers: Use compliant authentication systems and archive digital records responsibly.

4. Freedom of Information Act, 1999 (Revised 2016)
Purpose: Provides access to public documents and ensures transparency.
Scope: Applies to all state entities, with some exemptions.
Key Points:
• Includes clear request timelines and appeal rights.
• Expanded exemptions for national security and central banking.
For Data Producers: Respond to FOI requests within 30 days, apply exemption lists, and publish agency data online.

Appendix 1: Country source websites

1. ATG	Data Protection Electronic Transactions Electronic Crimes Freedom of Information	https://laws.gov.ag/laws/
2. BHS	Computer misuse (2003) Data Protection Electronic communications & transactions Freedom of Information	https://www.commonlii.org/ https://laws.bahamas.gov.bs/cms/legislation.html
3. BRB	Computer Misuse Act (2005) Cybercrime Bill (2024)	https://cmabarbados.com/ https://www.barbadosparliament.com/bills/details/741
	Data Protection Freedom of information	https://www.privacylaws.com/media/4517/data-protection-act-2019-29.pdf www.oas.org/sap/dgpe/acceso/docs/Barbados2008
4. BLZ	Cybercrime Act 2020[6] Data Protection Electronic transactions Freedom of information	https://www.agm.gov.bz/laws/act
5. DMA	Data protection	NONE https://www.uwi.edu/data-protection/pg-external_dominica.php Some elements of privacy covered by constitution[1]
	Electronic transactions	https://dominica.gov.dm/laws-of-dominica
	Computer misuse Cybercrimes -	NONE https://dpocaribbean.com/cybercrime-laws
	Freedom of information	Can't find one but need ref
6. GRD	Data Protection (2023) Electronic Transactions (2013) Electronic Crimes Act 2013[2] Amended 2014	https://laws.gov.gd
	Freedom of Information	Not on govt website
7. GUY	Cybercrime Act 2018[6] Data protection Electronic transactions Freedom of information	https://www.parliament.gov.gy/publications/acts-of-parliament/
8. HTI	Computer misuse Cybercrimes -	NONE https://dpocaribbean.com/cybercrime-laws
	Data protection	
	Electronic transactions	
	Freedom of information	
9. JAM	Cybercrimes Act, 2015[6]	https://laws.moj.gov.jm/library/act-of-parliament/31-of-2015-the-cybercrimes-act-final
	Data protection act 2020	https://laws.moj.gov.jm/library/act-of-parliament/7-2020-the-data-protection-act
	Electronic Transactions Act 2007 Updated 2014	https://laws.moj.gov.jm/library/statute/the-electronic-transactions-act
	Access to information	https://laws.moj.gov.jm/library/act-of-parliament/no-21-the-access-to-information-act-2002
10. MSR	Montserrat Penal Code (Amendment) Act, 2022[6]	https://www.gov.ms/wp-content/uploads/2024/08/Act-No.-22-of-2024-Penal-Code-Amendment-Act.pdf
		https://www.gov.ms/government/legal-department/attorney-generals-chambers/acts-passed-2018-2020/
11. KNA	Data Protection (2018)	https://lawcommission.gov.kn/

[1] https://www.uwi.edu/data-protection/pg-external_dominica.php
[2] https://dpocaribbean.com/cybercrime-laws

	Electronic Crimes 2017 Freedom of information (2024) Amended Enacted 2018 Electronic transaction 2017 revised	
12. LCA	Data Protection Act (2015)	http://attorneygeneralchambers.com/laws-of-saint-lucia/data-protection-acthttps://npc.govt.lc/laws/acts/2015 https://npc.govt.lc/laws/acts/2011
	Computer Misuse (2011)	http://attorneygeneralchambers.com/laws-of-saint-lucia/computer-misuse-act https://npc.govt.lc/laws/acts/2011
	Electronic Transactions (2015)	http://attorneygeneralchambers.com/laws-of-saint-lucia/electronic-transaction-act https://npc.govt.lc/files/laws/acts/2014/Act%20No.%206%20of%202014%20-%20Electronic%20Transactions%20(Amendment)%20Act%20-%20Price%20$2.00.pdf
	Freedom of Information	NONE
13. VCT	Data Protection Act (2003)	https://www.theinformationcollective.com/dpl/st-vincent-and-the-grenadines-the-privacy-act
	Electronic Transactions (2007)	https://etasvg.com/St-Vincent-Grenadines-Electronic-Transactions-Act-2015.pdf
	Computer Misuse/cybercrime Bill	https://assembly.gov.vc/assembly/images/stories/cybercrime%20bill%202016.pdf
	Freedom of information (2003)	https://observatoriop10.cepal.org/sites/default/files/documents/vc_-_freedom_of_information_act_2003.pdf
14. TTO	Data Protection Act (2011) amended 2016	https://laws.gov.tt/ttdll-web/revision/list
	Computer Misuse Act 2000 last amended 2016	https://laws.gov.tt/ttdll-web/revision/list
	Electronic transaction 2011 amended 2016	https://laws.gov.tt/ttdll-web/revision/list
	Freedom of information 1999 last amended 2003	https://laws.gov.tt/ttdll-web/revision/list