

From Laws to Practice

Strengthening Data Protection Authorities in the Caribbean



From Laws to Practice

Strengthening Data Protection Authorities in the Caribbean

ABOUT DPO Caribbean

DPO Caribbean is dedicated to advancing digital policy solutions for the Caribbean. We support governments, institutions, and stakeholders in navigating the social, economic, privacy and security challenges of the digital age. Through evidence-based research, policy analysis, and regional collaboration, we provide advisory services in digital services, data protection, cybersecurity, and AI governance, helping to shape inclusive, resilient, and future-ready digital frameworks that protect citizens and enable sustainable digital transformation across the Caribbean.

Visit us at <https://dpocaribbean.com/>

AUTHOR

Corlane Barclay, PhD, PMP, LLB, CLE

Principal Consultant, DPO Caribbean

services@dpocaribbean.com

Please cite this publication as:

DPO Caribbean (2026), *From Laws to Practice: Strengthening Data Protection Authorities in the Caribbean*, DPO Caribbean, Jamaica, DOI: 10.13140/RG.2.2.26175.68001

© June 2026 DPO Caribbean, all rights reserved

ISBN 978 976 97440 3 5

Table of Contents

Executive Summary	vi
Introduction.....	1
<i>The Implementation Gap</i>	<i>1</i>
<i>Current Regional Outlook</i>	<i>2</i>
<i>Purpose of the Report.....</i>	<i>2</i>
<i>Towards Effective Data Governance</i>	<i>2</i>
Methodology	3
Evolution of Regional Data Governance Initiatives	5
Status of Data Protection Laws in the Caribbean.....	7
Supervising Authority	11
<i>Defining Supervisory Authority</i>	<i>11</i>
<i>Conditions for Effective Supervisory Authorities</i>	<i>11</i>
Tenure and Security of Tenure.....	12
Nature of Appointment.....	12
Qualifications, Expertise, and Professional Competence	13
Duty of Confidentiality and Professional Secrecy.....	13
Independence	14
Access to Resources	14
<i>Powers and Functions</i>	<i>14</i>
Compliance Monitoring, Investigations and Enforcement	14
Complaints Handling and Redress	15
Advisory Function	16
Public Awareness and Education	16
Legislative and Policy Review	17
Research and Technology Monitoring	17
Cooperation	17
Stakeholder Engagement	17
Accountability and Reporting	17
<i>Conclusion</i>	<i>18</i>
Regional DPA Legislative Frameworks.....	19
<i>Institutional Conditions</i>	<i>19</i>
Tenure and Security of Tenure.....	19
Nature of Appointment.....	19
Qualifications, Expertise, and Professional Competence	20
Duty of Confidentiality and Professional Secrecy.....	20
Independence	20
Resource Capability	21
<i>Functional Capabilities of Supervisory Authorities</i>	<i>21</i>
Compliance Monitoring, Investigation and Enforcement	21

Complaints Handling and Redress	22
Advisory Function	22
Public Awareness and Education	22
Legislative and Policy Review	22
Research and Technology Monitoring	23
Cooperation (Domestic and International)	23
Stakeholder Engagement	23
Accountability and Reporting	24
<i>Conclusion</i>	24
A Legislative and Operational Maturity Model for Supervisory Authorities.....	27
<i>Tier 5: Pre-Established</i>	28
<i>Tier 4: Establishing</i>	28
<i>Tier 3: Operating</i>	29
<i>Tier 2: Evolving</i>	29
<i>Tier 1: Maturing</i>	30
<i>Conclusion</i>	31
Policy Recommendations.....	32
<i>Strategic Policy Direction</i>	32
<i>Enhance Legal and Regulatory Frameworks</i>	32
<i>Prioritise Institutional Strengthening</i>	33
<i>Foster Functional Effectiveness</i>	34
<i>Encourage Regional Cooperation and Integration</i>	35
<i>Nurture Stakeholder Engagement</i>	35
<i>Implementation Priorities</i>	36
Conclusion	37
 List of Tables	
Table 1: Summary of Key Data Governance Projects.....	5
Table 2: State of Data Protection Regimes in CARICOM.....	8
Table 3: Caribbean Countries with Data Protection Enactments.....	9
Table 4: Functional Dimensions of Data Protection Supervisory Authorities	15
Table 5: Regional Supervisory Authorities: Dimensional Summary of Alignment with Modern Legal Standards	25
Table 6: Comparative Assessment of Legislative Frameworks to Support DPAs	26
 List of Figures	
Figure 1: Summary Status of Data Protection Laws in the Caribbean	7
Figure 2: Summary Status of DPAs in the Caribbean	8
Figure 3: Conditions for Effective SAs	12
Figure 4: Legislative and Operational Maturity Model	27
Figure 5: Regional Maturity Mapping	29

Executive Summary

This report provides a comprehensive assessment of the state of data protection governance in the Caribbean, with a particular focus on the design, capacity, and effectiveness of supervisory authorities. As digital transformation accelerates across economies, the ability of jurisdictions to establish credible, independent, and well-resourced oversight mechanisms has become a defining feature of regulatory legitimacy, cross-border data flows, and international trust. In this context, the report benchmarks regional frameworks against global standards, most notably those reflected in the EU General Data Protection Regulation (GDPR), to evaluate both legislative alignment and operational readiness.

From Fragmentation to Emerging Convergence

Over the past decade, Caribbean jurisdictions have made notable progress in advancing data governance frameworks. This evolution reflects a broader shift from fragmented models toward more comprehensive data protection regimes. Several countries have enacted standalone legislation or modernised existing frameworks, signalling growing recognition of privacy as both a fundamental right and an economic enabler.

However, the pace and depth of reform remain uneven. While some jurisdictions have developed relatively sophisticated legal and institutional architectures, others continue to rely on partial or transitional arrangements. The result is a heterogeneous regional landscape, where formal legislative convergence does not always translate into functional equivalence or regulatory effectiveness.

Supervisory Authorities: The Critical Implementation Gap

At the core of this assessment is the role of supervisory authorities as the primary vehicles for enforcing data protection law. The report finds that while several Caribbean statutes incorporate key GDPR-inspired principles, the effectiveness of these regimes ultimately depends on the institutional strength and operational capacity of their supervisory authorities.

The analysis identifies two interdependent pillars that determine institutional maturity:

1. Institutional Conditions

Effective supervisory authorities require:

- Clearly defined tenure and protection from arbitrary removal
- Transparent and merit-based appointment processes
- Adequate professional qualifications and technical expertise
- Strong confidentiality obligations
- Structural independence from political or administrative interference
- Sufficient financial, technical and human resources

Across the region, these conditions are inconsistently realised. While some jurisdictions demonstrate robust safeguards, particularly in relation to independence and tenure, others exhibit vulnerabilities, including executive influence over appointments, limited statutory clarity, and constrained resourcing.

2. Functional Capabilities

Beyond institutional design, supervisory authorities must be empowered to act. Core functions assessed include:

- Compliance monitoring, investigations, and enforcement
- Complaints handling and access to redress
- Advisory and guidance roles
- Public awareness and education initiatives
- Legislative and policy review
- Research and monitoring of technological developments
- Domestic and international cooperation
- Stakeholder engagement
- Accountability and reporting mechanisms

The findings reveal that functional capabilities are generally more developed than institutional safeguards, with many authorities possessing broad mandates on paper. However, enforcement powers and investigative tools are not always matched by the operational capacity to deploy them effectively.

A Regional Legislative and Operational Maturity Model

To synthesise these findings, the report introduces a five-tier maturity model, capturing the legislative and operational progression of supervisory authorities from nascent to fully operational systems:

- **Tier 1: Maturing:** Fully developed, independent, and functionally robust authority aligned with global best practice
- **Tier 2: Evolving:** Expanding powers, increasing institutional maturity
- **Tier 3: Operating:** Authority is functional with basic capabilities
- **Tier 4: Establishing:** Legislative framework exists but is not operationalised
- **Tier 5: Pre-Established:** No active supervisory authority or enabling framework

Application of this model highlights a clear regional pattern:

- Several are in the operating stages, with meaningful progress but persistent institutional or capacity gaps
- The majority remain in pre-established or establishing phases, where implementation has yet to occur or remains incomplete
- No country has reached the highest maturity tier, reflecting limited experience and the requisite institutional capacity required to achieve full maturity

While the maturity model is tailored to the Caribbean regional context, its underlying structure is transferable. It can be readily adapted to other emerging data protection jurisdictions and applied across different regulatory domains.

Key Insights

The examination yields several insights, including the following:

1. **Legislation alone is insufficient**
The existence of a data protection law does not guarantee effective regulation. Institutional independence and operational capacity are decisive.
2. **Institutional weaknesses constrain functional effectiveness**
Even where enforcement powers are strong on paper, weak governance structures limit impact on the regulatory ecosystem.
3. **Accountability mechanisms are uneven**
Regular reporting, parliamentary oversight, and transparency obligations are not consistently embedded across jurisdictions.
4. **Resource constraints remain a systemic challenge**
Many supervisory authorities face limitations in staffing, funding, and technical expertise, affecting their ability to perform core functions. This is despite the legislative provisions, at least in part, to support institutional capacity.
5. **Regional convergence is emerging but incomplete**
While GDPR-inspired frameworks are increasingly common, full functional equivalence remains limited to a small number of jurisdictions.

Policy Implications and Way Forward

To advance toward internationally credible data protection regimes, the report underscores the need for a shift from legislative adoption to operationalisation. Key priorities include:

- Strengthening legal guarantees of independence and tenure
- Ensuring transparent and merit-based appointment processes
- Securing sustainable funding and technical capacity
- Enhancing enforcement mechanisms and investigative tools
- Institutionalising accountability through regular reporting and oversight
- Promoting regional cooperation and knowledge-sharing

A coordinated regional approach could accelerate progress, reduce fragmentation, and enhance the Caribbean's position in the global data economy.

Final Thoughts

The Caribbean stands at a pivotal moment in the development of its data governance frameworks. Significant legislative strides have been made, but the transition from legislative convergence to effective enforcement remains incomplete. Strengthening supervisory authorities, both institutionally and functionally, will be central to closing this gap.

Achieving this will not only safeguard individual rights but also enable greater participation in cross-border data flows, support digital innovation, and reinforce trust in the region's regulatory environment.

Introduction

Over the past decade, the Caribbean has undergone a significant transformation in its data governance landscape, driven by national digital transformation agendas and an increasing recognition of the need to regulate the processing of personal data. As economies across the region become more digitally integrated, data protection has emerged as both a regulatory necessity and a strategic enabler of trust, innovation, and cross-border economic participation.

This evolution has been supported by a range of internationally backed initiatives, including HIPCAR (Enhancing Competitiveness in the Caribbean through the Harmonisation of ICT Policies, Legislation and Regulatory Procedures), EGRIP (E-Government for Regional Integration Project), and CARDTP (Caribbean Digital Transformation Project). These programmes have played an important role in shaping legislative development and promoting a degree of regional coherence in data governance approaches.

The introduction of the General Data Protection Regulation (GDPR) has had a profound influence on the design of data protection frameworks globally, including in the Caribbean. As a widely recognised benchmark, the GDPR has informed legislative drafting across several jurisdictions in the region. Illustratively, countries such as Jamaica, Barbados, Belize, and Guyana have enacted data protection laws that reflect core GDPR principles, including rights-based protections, accountability obligations, and regulatory oversight mechanisms. At the same time, other jurisdictions, including the Bahamas and several members of the Organisation of Eastern Caribbean States (OECS), are in various stages of updating and modernising their legislative frameworks.

The Implementation Gap

Notwithstanding this legislative progress, it becomes clear that the enactment of data protection laws is only an initial step in establishing effective governance systems. A persistent gap often exists between formal legal frameworks and their practical implementation. As highlighted by an OECD Report¹, many countries that have enacted data protection legislation continue to face weak enforcement, limited regulatory independence, and underdeveloped policy implementation.

In the Caribbean, this gap is most evident in relation to Data Protection Authorities (DPAs), which are central to ensuring oversight, accountability, and enforcement. Although many jurisdictions have provided for such authorities in law, their establishment and effective operation are frequently constrained by limited institutional capacity, operational readiness, technical expertise, and financial resources. Further, earlier initiatives, including the development of model privacy legislation under the HIPCAR and EGRIP projects, achieved limited adoption and did not consistently lead to the establishment of operational supervisory authorities. As a result, a significant number of DPAs remain non-operational, while a few are operating with limited reach and impact.

The current wave of GDPR-inspired reforms therefore presents a critical juncture. Without corresponding investment in institutional capacity and operational systems, there is a risk that modern legislative frameworks may not translate into effective regulatory practice.

¹ OECD (2021), Development Co-operation Report 2021: Shaping a Just Digital Transformation, OECD Publishing, Paris, <https://doi.org/10.1787/ce08832f-en>.

Current Regional Outlook

Available data, grounded in our *State of Data Protection and Privacy Laws in the Caribbean Report*², underscores the extent of this implementation gap. Among selected Caribbean jurisdictions (14) with enacted data protection legislation:

- Approximately 64% have brought their laws into force, at least in part
- Only 36% have supervisory authorities that are operational to any degree
- Just 21% have fully functioning regulators

These figures indicate that, in practical terms, fewer than one in four jurisdictions currently benefits from a fully operational data protection authority, while in most cases the designated regulator remains either partially established or non-operational.

Purpose of the Report

Against this background, this report examines the development and effectiveness of data protection frameworks in the Caribbean, with a particular focus on supervisory authorities. It seeks to move beyond a purely legislative analysis to assess how these authorities function in practice.

Specifically, the report:

- Examines the current landscape of data protection laws and the functioning of active data protection authorities
- Analyses the institutional conditions underpinning supervisory authorities
- Evaluates their functional capabilities and regulatory powers
- Identifies gaps between statutory provisions and operational reality
- Develops a maturity model to assess levels of institutional and operational development
- Provides recommendations to support the strengthening of supervisory authorities across the region

Towards Effective Data Governance

This report advances the view that effective data protection in the Caribbean will depend not only on the existence of modern legal frameworks, but on the establishment of supervisory authorities that are independent, adequately resourced, and operationally capable.

Strengthening these institutions will be critical to enhancing regulatory credibility, supporting cross-border data flows, and positioning the region within the evolving global data governance landscape.

² C. Barclay, 2024, *The State of Data Protection and Privacy Laws in the Caribbean*, DPO Caribbean, DOI: 10.13140/RG.2.2.33510.19527/1

Methodology

To achieve the stated objectives, the report adopts a structured methodology combining desk-based research and comparative legal and policy analysis, supported by systematic analytical and design frameworks. This multi-dimensional approach enables an assessment of not only the formal characteristics of data protection regimes but also the extent to which supervisory authorities are operational and effective in practice.

Desk Review

The study is grounded in a comprehensive desk review of primary and secondary sources. Primary materials include enacted legislation, draft bills, and official policy documents across Caribbean jurisdictions. Where available, these are supplemented by regulatory guidance, annual reports, and other published outputs of data protection authorities. Secondary sources, including regional policy instruments and relevant academic and institutional literature, are also incorporated to provide contextual depth. This component supports a baseline assessment of the legal and institutional landscape and informs the analysis of both legislative development and the functioning of supervisory authorities.

Comparative Legal and Policy Analysis

A qualitative comparative approach is applied to examine patterns of convergence and divergence across jurisdictions. More than twenty Caribbean jurisdictions are reviewed at a regional level to establish an overview of legislative adoption and reform trajectories. From this group, a subset of jurisdictions is selected for detailed analysis based on criteria such as legislative status and relevance to the study. The selected frameworks are analysed in depth to assess institutional arrangements, governance structures, and the scope of regulatory powers. This enables a systematic evaluation of the conditions underpinning supervisory authorities and their capacity to perform core functions.

Analytical Framework

To ensure consistency and comparability, the analysis is guided by a structured dimensional framework framed through the lens of key elements of modern supervisory authority architecture. Each jurisdiction is assessed across key regulatory domains spanning institutional conditions and functional capabilities, which facilitates the identification of gaps between statutory provisions and operational reality.

Benchmarking Against Global Standards

The assessment is further contextualised against established international standards, particularly those reflected in the GDPR. This benchmarking exercise provides a reference point for evaluating the robustness and completeness of national frameworks, especially in areas such as institutional independence, enforcement authority, and accountability. While acknowledging differences in legal systems and resource constraints, this comparative lens supports a more rigorous assessment of alignment with global good practices.

Maturity Model Development

Building on the comparative analysis, the report develops a maturity model to classify jurisdictions according to their level of institutional and operational development. Principles of standard maturity model development frameworks³ are used as a reference point to aid in the model design. The model reflects a progression from nascent frameworks to more advanced stages characterised by functional enforcement, institutional independence, and sustained regulatory activity.

Limitations

The methodology is subject to certain limitations. As a desk-based exercise, it relies on publicly available information, which may vary in scope, quality, and timeliness across jurisdictions. Consequently, while the analysis provides a robust assessment of legal frameworks and institutional design, it may not fully capture the nuances of implementation in practice.

³ See for example, Barclay, C. (2014, June). Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model (CM 2). In Proceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world-Impossible without standards? (pp. 275-282). IEEE.

Evolution of Regional Data Governance Initiatives

The evolution of data protection and digital governance in the Caribbean has been shaped by a sequence of interconnected regional initiatives, each reflecting a shift in scope from legal harmonisation to institutional implementation and, most recently, to comprehensive digital transformation (Table 1).

The HIPCAR initiative⁴, led by institutions such as the International Telecommunication Union (ITU), the Caribbean Community (CARICOM), and the Caribbean Telecommunications Union (CTU), focused primarily on regional legal harmonisation of ICT frameworks. Its core output was the development of model legislation across key areas, including data protection, cybercrime, e-transactions, and e-commerce. HIPCAR played a foundational role in embedding core data protection principles into regional legal discourse, but its impact was largely normative, with limited institutional implementation.

Building on this foundation, the EGRIP programme (e-Government for Regional Integration Project)⁵, supported by the World Bank and the OECS Commission, shifted the emphasis from legal harmonisation to digital government implementation and interoperability across OECS member states. Its focus was on strengthening public sector efficiency through shared e-government systems such as e-tax platforms, e-ID frameworks, and interoperability standards. While not primarily a data protection initiative, EGRIP introduced significant data-intensive systems, indirectly advancing the need for structured data governance and supporting draft legislative development in areas such as data protection and cybercrime.

The most recent phase, the CARDTP initiative⁶, represents a broader and more integrated approach to end-to-end digital transformation. Also supported by the World Bank and regional institutions, including the OECS Commission and CARICOM Implementation Agency for Crime and Security (CARICOM IMPACS), CARDTP extends beyond government digitisation to include the development of the digital economy ecosystem. Its scope encompasses data governance, cybersecurity, digital identity systems, innovation frameworks, and digital skills development. In contrast to earlier initiatives, CARDTP places a stronger emphasis on enabling institutional capacity and trust infrastructure, positioning data protection and cybersecurity as central components of digital transformation.

These initiatives illustrate a clear trajectory in regional policy development, moving from HIPCAR's emphasis on model laws and regulatory harmonisation, to EGRIP's focus on interoperable digital government systems, and ultimately to CARDTP's more comprehensive digital economy and governance agenda. Within this continuum, data protection has shifted from a largely normative legal concept to an increasingly operational requirement embedded within broader digital transformation efforts. This evolution also appears to reflect a corresponding shift in the perspectives and maturity of development partners and donor agencies, particularly in their growing emphasis on implementation capacity, institutional strengthening, and sustainability rather than legislative adoption alone.

Table 1: Summary of Key Data Governance Projects

⁴ <https://caricom.org/projects/hipcar-project/>

⁵ <https://www.worldbank.org/en/results/2016/09/21/supporting-egovernment-systems-in-the-caribbean>

⁶ <https://oecs.int/en/our-work/knowledge/library/projects/caribbean-digital-transformation-project-cardtp>

Projects	Primary Objective	Lead Institutions	Focus Area	Primary Outcomes	Participating Countries
HIPCAR	Regional harmonisation of ICT legal and regulatory frameworks	ITU, CARICOM, CTU	ICT legal frameworks (data protection, cybercrime, e-transactions, e-commerce)	Model laws and harmonised legislative frameworks	CARIFORUM states
EGRIP	Improve efficiency, transparency, and interoperability of e-government systems in OECS states	World Bank, OECS Commission, national governments, regional ICT agencies	Digital government systems, interoperability frameworks (e-GEA, eGIF), and shared public services	Digital government infrastructure, interoperability standards, and public sector modernisation	OECS member states
CARDTP	End-to-end digital transformation of government, services, and digital economy	World Bank, OECS Commission, national governments, ECTEL, ECCB, CARICOM IMPACS	Digital economy ecosystem: data governance, cybersecurity, digital ID, innovation, and digital skills	Policy reform, capacity building, and strengthened digital economy and trust infrastructure	OECS/ECCU member states

Status of Data Protection Laws in the Caribbean

A review of the *State of Data Protection and Privacy Laws in the Caribbean* report⁷ highlights a persistent tension in the regional trajectory over the last decade, particularly. The data spotlights that while the pace of legislative adoption has accelerated, operationalisation of the laws and institutional implementation, particularly the establishment and effective functioning of Data Protection Authorities (DPAs), continues to lag significantly behind (Figure 1, Figure 2).

Summary: Status of Laws

- No enactment: 5 of 20 countries → 25%
- Draft stage: 1 country → 5%
- Enacted, not in force: 4 countries → 20%
- Partially in force: 4 countries → 20%
- Fully in force: 6 countries → 30%

Figure 1: Summary Status of Data Protection Laws in the Caribbean

There is clear evidence that data protection legislation is now widespread across CARICOM, with many jurisdictions having moved beyond policy intent to formal enactment (Table 2). This is evident in the growing number of countries that have enacted data protection legislation, many within the last decade and often influenced by modern regulatory models, such as the GDPR. However, this does not present the full picture.

Jurisdictions such as The Bahamas, Bermuda, and the Cayman Islands represent earlier adopters, with laws in force and supervisory authorities that are operational. In contrast, Antigua and Barbuda and Saint Kitts and Nevis have legislation fully in force, indicating that their legal frameworks are formally active through implicit and explicit commencement processes; however, their current regimes can be deemed inactive. While it reflects a broader regional shift toward the establishment of data protection regimes aligned with international practice, the divergence highlights a critical distinction between a law coming into force and institutional capability.

At the same time, a substantial number of countries fall within intermediate categories. Jurisdictions such as Belize, Guyana, Grenada, and Saint Lucia have enacted legislation that are not yet in force, while Jamaica, Barbados, and Trinidad and Tobago show partial or phased commencement. This distribution indicates that, although legislative frameworks are in place, the transition from enactment to full operational effect varies considerably across jurisdictions and, in some cases, remains ongoing.

A smaller set of countries, including Anguilla, Dominica, Haiti, Montserrat, and Turks and Caicos Islands, does not have clearly identified data protection legislation based on available public sources, while Suriname remains at the draft stage. These cases confirm that legislative development is still emerging or has yet to be initiated in parts of the region.

⁷ C. Barclay, 2024, *The State of Data Protection and Privacy Laws in the Caribbean*, DPO Caribbean, DOI: 10.13140/RG.2.2.33510.19527/1

Table 2: State of Data Protection Regimes in CARICOM

No Enactment	Draft	Enacted, Not in Force	Partially in Force	Fully in Force
Anguilla	Suriname	Belize	Barbados	Antigua and Barbuda
Dominica		Grenada	Jamaica	Bahamas
Haiti		Guyana	Trinidad and Tobago	Bermuda
Montserrat		Saint Kitts and Nevis		British Virgin Islands
Turks and Caicos Islands		Saint Lucia		Cayman Islands
				Saint Vincent and the Grenadines

Within the context of active supervisory bodies, Table 3 highlights a clear regional dilemma in which the gap between legal provision and institutional reality remains pronounced across a significant number of jurisdictions. In practice, only a limited subset of countries has successfully translated data protection legislation into fully functioning regulatory systems (Figure 2). For example, Antigua and Barbuda, Saint Lucia, and Saint Kitts and Nevis have laws formally in force, yet their designated supervisory authorities are not fully operational.

In other jurisdictions, including Belize, Guyana, and Grenada, data protection legislation has been enacted but remains non-operational, resulting in both legal and institutional frameworks that are effectively dormant in practice. This situation reflects a broader disconnect between legislative adoption and the development of the institutional capacity required for enforcement and oversight. A number of these jurisdictions, particularly within the OECS, are currently engaged in the CARDTP initiative, which is focused on supporting the development of harmonised data protection frameworks across the sub-region. For those countries, it is therefore anticipated that this will accelerate the transition from legislative enactment to effective regulatory implementation.

Summary: Status of DPAs

- Fully operational DPAs: 3 of 14 countries
(The Bahamas, Bermuda, Cayman Islands)
- Partially operational DPAs: 2 of 14 countries
(Barbados, Jamaica)
- Non-operational DPAs: 9 of 14 countries

Figure 2: Summary Status of DPAs in the Caribbean

Against this background, the analysis suggests that the landscape is characterised by a differentiated continuum of institutional and regulatory maturity. At one end are jurisdictions with operational regulators and functioning enforcement ecosystems; at the other are countries where legal frameworks remain largely aspirational, with limited or no operational effect. Between these poles sits a substantial middle tier in which the legal architecture is in place, but supervisory authorities are still in the process of being established, resourced, or fully empowered to discharge their mandates effectively.

The data also suggest that while legislative convergence has progressed relatively quickly, institutional convergence has been slower and more uneven. This distribution underscores an important shift in the regional data protection discourse. Earlier phases of reform focused primarily on legislative adoption, often measured by whether a country had enacted a data protection law. Today, the conversation should be centred on operationalisation: whether laws are in force, whether authorities are functional, and whether regulatory oversight is being meaningfully exercised.

A closer examination also highlights that the challenge is not confined to long-term capacity constraints. In many cases, the initial “getting off the ground” phase represents a critical bottleneck. The absence of commencement orders, delays in appointing commissioners, and difficulties in establishing basic administrative and technical infrastructure all point to structural and procedural barriers that arise at the earliest stages of implementation. Even where authorities are nominally established, limited staffing, unclear mandates or priorities, or insufficient funding can result in entities that exist in law but lack practical regulatory presence.

Within this context, the Caribbean experience reflects a broader global lesson that the effectiveness of data protection regimes depends not only on the substance of the law, but also on the existence of credible, independent, and operational supervisory institutions. The current regional landscape therefore calls for a reframing of priorities, from the continued proliferation of legislation to a more deliberate focus on building, resourcing, and sustaining Data Protection Authorities as functioning and effective regulators.

This report engages directly with that shift in emphasis. By mapping the varying levels of DPA maturity across the Caribbean and analysing the factors that shape their operational readiness, it seeks to contribute to a more grounded and implementation-focused understanding of data protection in the region.

Table 3: Caribbean Countries with Data Protection Enactments

Country	Legislation	Enactment Year	Law in Force	Regulatory Authority	Status of Authority
1. Antigua & Barbuda	Data Protection Act	2013	Yes	Data Protection Commissioner	Not operational
2. Bahamas	Data Protection (Privacy of Personal Information) Act	2003	Yes	Data Protection Commissioner	Fully operational
3. Barbados	Data Protection Act	2019	Yes, partially	Data Protection Commissioner	Partially operational
4. Belize	Data Protection Act	2021	No, (No commencement order ID)	Data Protection Commissioner	Not operational
5. Bermuda	Personal Information Protection Act (PIPA)	2016, 2023	Yes	Privacy Commissioner	Fully operational

Country	Legislation	Enactment Year	Law in Force	Regulatory Authority	Status of Authority
6. British Virgin Islands	Data Protection Act	2021	Yes	Information Commissioner	Fully operational
7. Cayman Islands	Data Protection Law	2017	Yes	Ombudsman	Fully operational
8. Grenada	Data Protection Act	2023	No, (No commencement order ID)	Information Commission	Not operational
9. Guyana	Data Protection Act	2023	No, (No commencement order ID)	Data Protection Office	Not operational
10. Jamaica	Data Protection Act	2020	Phased commencement via Ministerial Orders	Information Commissioner	Partially operational
11. Saint Kitts & Nevis	Data Protection Act	2018	No, (No commencement order ID)	Information Commissioner	Not operational
12. Saint Lucia	Data Protection Act	2011, 2023	No, (No commencement order ID)	Data Protection Commissioner	Not operational
13. Saint Vincent & Grenadines	Privacy Act	2003	Yes	Privacy Commissioner	Not operational
14. Trinidad & Tobago	Data Protection Act	2011	Yes, partially	Information Commissioner	Not operational

Supervising Authority

Defining Supervisory Authority

A supervisory authority is an independent public body responsible for overseeing the application and enforcement of a national data protection framework. Its core role is to ensure compliance, safeguard the rights of data subjects, facilitate the free flow of data, and provide regulatory oversight through a combination of monitoring, guidance, and enforcement functions.

Globally, the institutional design of such authorities has evolved over time. In a number of earlier or hybrid models, data protection oversight was combined with broader transparency mandates under freedom of information or access to information regimes. This gave rise to the “Information Commissioner” model, where a single office is responsible for both privacy and access to information. For example, in the United Kingdom, the Information Commissioner’s Office (ICO)⁸ serves as the independent supervisory authority responsible for enforcing both data protection legislation under the UK General Data Protection Regulation and the Data Protection Act 2018, as well as information rights legislation, including the Freedom of Information Act 2000. The ICO therefore operates as a unified regulator for both privacy and access to information, combining oversight of personal data protection with transparency and public access to information within a single institutional framework. Australia adopts a broadly similar framework, with the Office of the Australian Information Commissioner (OAIC)⁹ serving as the independent regulator responsible for both privacy and information access functions, including oversight of the Privacy Act 1988 and freedom of information legislation.

More recent international practice, particularly in jurisdictions influenced by the GDPR, has moved toward dedicated data protection authorities with clearly defined mandates, enhanced enforcement powers, and stronger institutional independence.

For the purposes of this report, the term “supervisory authority” refers to the body responsible for oversight of the personal data protection regime, whether it operates as a standalone authority or within a broader institutional framework. This approach allows for consistent comparative analysis across jurisdictions with differing institutional models, while recognising the historical and structural factors that have shaped their development.

Conditions for Effective Supervisory Authorities

The effectiveness of a data protection supervisory authority is closely tied to the legal and institutional conditions under which it operates. International standards, particularly those reflected in the EU framework, emphasise that independence, competence, and capacity are not merely formal requirements, but foundational to credible and effective regulation.

⁸ <https://ico.org.uk/about-the-ico/who-we-are/decision-making-structure/>

⁹ <https://www.oaic.gov.au/about-the-OAIC/what-we-do>

These provisions establish a coherent standard, wherein supervisory authorities must be independent in law, secure in tenure, competent in expertise, bound by confidentiality, and adequately resourced. Where any of these conditions are weak or absent, there is a risk that authorities will exist formally but lack the operational capability to deliver meaningful regulatory oversight.

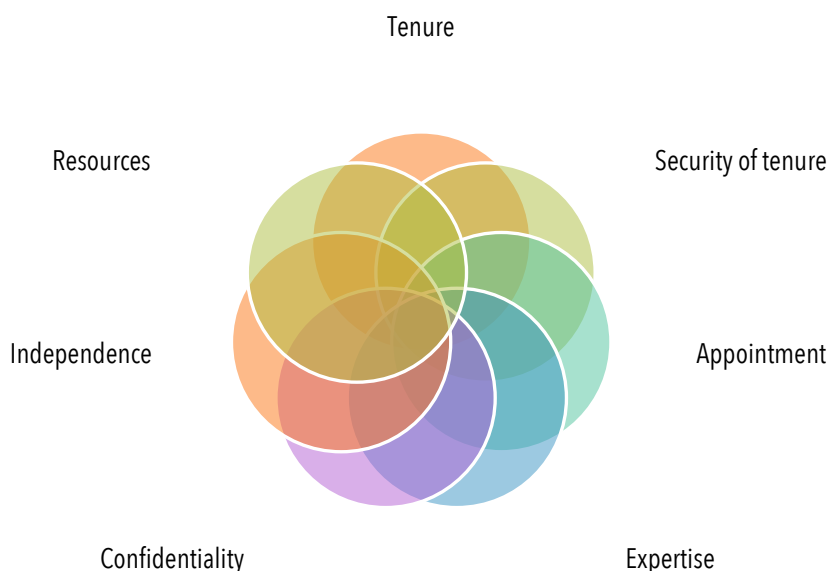


Figure 3: Conditions for Effective SAs

Tenure and Security of Tenure

A fixed and sufficiently long tenure is a key safeguard of independence. According to Article 54(1)(d) of the GDPR¹⁰, for example, members of supervisory authorities must serve for a term of not less than four years, providing continuity and insulation from short-term political influence. In practice, many jurisdictions adopt terms of five years or more, often with the possibility of renewal.

Equally important is security of tenure; removal should be limited to clearly defined grounds such as incapacity or serious misconduct. This protects the office-holder from arbitrary dismissal and reinforces regulatory autonomy. The approach is reflected in jurisdictions such as the United Kingdom, Australia and Canada, where the supervisory authority benefits from statutory protections that limit removal and support institutional stability.

Nature of Appointment

Appointment processes play a critical role in safeguarding the independence and legitimacy of supervisory authorities. International good practice favours transparent, merit-based appointments, typically involving the Head of State or a

¹⁰ <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

structured process with executive nomination and some form of parliamentary or institutional oversight. This helps to balance executive influence while reinforcing public confidence in the regulator.

Comparative practice illustrates different but converging approaches. In Canada, the Privacy Commissioner is appointed by the Governor in Council following approval by both Houses of Parliament, embedding a dual executive-legislative process that strengthens accountability and independence. Similarly, in Australia, the Australian Information Commissioner is appointed by the Governor-General, with the process grounded in statutory criteria and public service appointment standards, supporting transparency and merit-based selection.

These approaches align with the principles reflected in the GDPR, particularly Article 53, which requires that members of supervisory authorities be appointed through a transparent procedure by parliament, government, the head of state, or an independent body.

Across jurisdictions, the underlying objective remains consistent, which is to ensure that supervisory authorities are insulated from undue political direction while maintaining democratic legitimacy and public trust.

Qualifications, Expertise, and Professional Competence

Effective supervision in today's complex data environments requires multidisciplinary expertise, integrating legal, technological, and regulatory knowledge. Modern supervisory authorities are expected to demonstrate specialised competence in data protection law, information technology, and regulatory practice. While Article 53 of the GDPR does not prescribe detailed qualification criteria, it requires that members possess the qualifications, experience, and skills, particularly in the field of personal data protection, necessary to perform their duties and exercise their functions.

In practice, this standard reflects the increasingly technical nature of data governance. Effective oversight now depends on an understanding of cybersecurity, digital systems, emerging technologies, and regulatory policy. Institutions such as the Information Commissioner's Office illustrate this multidisciplinary model, combining legal analysis with technical and policy expertise in their supervisory approach.

Accordingly, expertise should not be treated as a discretionary attribute but as a foundational statutory requirement, essential to ensuring both the effectiveness and credibility of the supervisory authority.

Duty of Confidentiality and Professional Secrecy

A further core condition is the obligation of professional secrecy, both during and after the term of office. This ensures that sensitive personal data, commercial information, and investigative materials handled by the authority are protected. The obligation of professional secrecy is codified under Article 54(2) of the GDPR, which requires that members and staff of supervisory authorities are bound by confidentiality obligations both during and after their term of office. This is critical to maintaining trust, particularly given the sensitive nature of personal data, commercial information, and investigative material handled by these authorities.

Notably, professional secrecy serves as a core institutional safeguard, extending beyond general confidentiality to impose strict limitations on the use and disclosure of information obtained in the course of regulatory functions. In this sense, it complements transparency and accountability by ensuring that, while supervisory authorities operate openly, sensitive information is handled with the necessary integrity and restraint required to maintain trust and protect regulated entities and individuals alike.

Independence

Independence is the cornerstone of effective supervision and thereby a key requirement of many mature regimes, such as GDPR. The principle of independence articulated in Article 52(1) requires supervisory authorities to act with complete independence in performing their tasks and exercising their powers, free from external influence. This reduces the risk of political and other external interference, enabling the supervisory authority to carry out its mandate independently and without undue influence.

Access to Resources

The importance of resources in establishing and maintaining an effective body cannot be overstated. This is reinforced by Article 52(4), which mandates that authorities be provided with the human, technical, and financial resources necessary to perform their functions effectively. Thus, adequate resourcing includes budgetary autonomy, staffing, and access to technical expertise. This is reflected in the practice of many mature regimes, where it is well established that the effectiveness of national supervisory authorities ultimately depends on sustained investment in institutional capacity, including technical and administrative capability as well as a robust enforcement infrastructure.

Powers and Functions

Supervisory authorities are conceived not merely as enforcement bodies, but as multi-functional institutions that integrate regulatory, advocacy, and policy advisory roles, as reflected in their governing legislation.

Examining the GDPR framework reinforces this multifaceted structure. Across modern data protection regimes, these functions are also increasingly standardised. The discussion below outlines each functional dimension in general terms, using the GDPR, particularly Articles 57 and 58, as a reference point for contemporary regulatory design (Table 4).

Compliance Monitoring, Investigations and Enforcement

Supervisory authorities are fundamentally responsible for ensuring that data protection laws are effectively applied in practice. This involves monitoring compliance, identifying breaches, and taking corrective or punitive action where necessary. In mature regulatory systems, this function is not passive or purely reactive but is supported by investigatory and sanctioning powers.

Under the GDPR, Article 57(1)(a) establishes the duty to monitor application of the Regulation, while Article 58(1) – (2) provides extensive investigative and corrective powers, including access to information, audits, warnings, reprimands, and orders to restrict or suspend processing.

Complaints Handling and Redress

A core function of supervisory authorities is to provide an accessible mechanism for individuals to lodge complaints and seek redress where their data protection rights are infringed. This is central to the protection of individual rights. This further ensures that enforcement is not solely state-driven but also responsive to individual grievances.

The GDPR explicitly reflects this in Article 57(1)(f), which requires authorities to handle complaints and inform data subjects of progress and outcomes. Complementary powers under Article 58(2) enable authorities to impose corrective measures such as rectification, erasure, or restriction of processing, thereby linking complaint-handling directly to enforceable remedies.

Table 4: Functional Dimensions of Data Protection Supervisory Authorities

Dimension	General Description	Legislative Approach (GDPR Reference)
1. Compliance Monitoring, Investigation & Enforcement	Continuous oversight of how organisations apply data protection law, including detection of breaches, investigation of complaints, and enforcement of corrective measures.	Article 57(1)(a) requires monitoring application of GDPR. Article 58(1)–(2) provides investigatory powers (access, audits) and corrective powers (warnings, reprimands, orders, fines via national law).
2. Complaints Handling & Redress	Mechanism for individuals to lodge complaints regarding misuse or unlawful processing of personal data, with follow-up and remedies.	Article 57(1)(f) mandates handling complaints and informing data subjects. Article 58(2)(b)–(g) enables binding corrective actions such as rectification, erasure, restriction, and notification.
3. Advisory Function	Includes providing guidance to controllers, processors, and public authorities on compliance obligations and interpretation of data protection rules.	Article 57(1)(c)–(d) requires advisory support to institutions and stakeholders. Article 58(3)(b) allows issuing opinions, advice, and recommendations.
4. Public Awareness & Education	Promoting understanding of data protection rights and obligations among the public and organisations to improve compliance culture.	Article 57(1)(b) requires raising awareness and understanding of risks, rights, and safeguards relating to personal data processing.
5. Legislative & Policy Review	Reviewing draft legislation, policies, and administrative measures to ensure alignment with data protection principles and rights.	Article 57(1)(c) and broader interpretive role allow input on legislative and administrative measures affecting data protection.
6. Research & Technology Monitoring	Tracking developments in technology and data processing practices to assess emerging risks and regulatory implications.	Article 57(1)(i) mandates monitoring relevant technological and societal developments impacting data protection.
7. Cooperation	Includes engaging with other supervisory authorities to ensure consistent enforcement	Articles 57(1)(g) and 60–62 establish structured cooperation mechanisms, mutual assistance, and consistency procedures.

Dimension	General Description	Legislative Approach (GDPR Reference)
	and address cross-border data processing issues.	
8. Stakeholder Engagement	Interaction with industry, civil society, and the public to inform regulatory guidance and ensure participatory governance.	Embedded across Article 57(1)(c), (d), and (e) through consultation, advisory processes, and engagement with controllers and data subjects.
9. Accountability & Reporting	Ensuring transparency through reporting to parliament/government and publishing findings, decisions, and annual reports.	Article 59 requires annual reporting to national parliaments. Institutional independence and accountability safeguarded under Articles 52–53.

Advisory Function

Supervisory authorities also serve an advisory role, guiding public bodies, private entities, and policymakers on the interpretation and application of data protection law. This function is preventive in nature, aimed at reducing non-compliance before it occurs.

Under the GDPR, Article 57(1)(c) and (d) requires supervisory authorities to advise controllers, processors, and public institutions on compliance obligations and data protection risks. This function is reinforced by Article 58(3)(b), which empowers authorities to issue opinions and recommendations. The Singapore Personal Data Protection Act¹¹ adopts an even more explicit approach, expressly providing for the delivery of consultancy, advisory, technical, managerial, and other specialist services relating to data protection. These provisions underscore that effective data protection regimes depend not only on enforcement powers but also on the proactive advisory capacity of supervisory authorities to guide compliance, mitigate risks early, and foster a culture of accountability.

Public Awareness and Education

Modern supervisory authorities are expected to promote awareness of data protection rights and obligations among the public and organisations. This function supports broader compliance by ensuring that rights are understood and enforceable in practice.

The GDPR addresses this in Article 57(1)(b), requiring authorities to promote public awareness and understanding of risks, rights, and safeguards. According to the Singapore Data Protection Act, this may include organising and conducting seminars, workshops, and symposia. This positions supervisory authorities as both regulators and educators, contributing to a culture of compliance.

¹¹ <https://sso.agc.gov.sg/Act/PDPA2012>

Legislative and Policy Review

Another important function is the review of proposed legislation, policies, and administrative measures to ensure alignment with data protection principles. This allows supervisory authorities to influence legal and policy development beyond enforcement.

Under the GDPR, Article 57(1)(c) enables advisory input into legislative and administrative measures, while broader institutional engagement ensures that data protection considerations are integrated into policy development. This reflects a preventive governance function aimed at mainstreaming data protection.

Research and Technology Monitoring

Supervisory authorities are also expected to monitor technological and societal developments that may affect data protection, ensuring that regulatory frameworks remain responsive to innovation and emerging risks.

The GDPR reflects this in Article 57(1)(i), which requires monitoring of relevant technological developments. This function is particularly significant in the context of digital transformation, artificial intelligence, and data-driven systems, where risks evolve rapidly.

Cooperation

Given the cross-border nature of data flows, supervisory authorities must cooperate with counterparts in other jurisdictions to ensure consistent enforcement and regulatory alignment.

The GDPR institutionalises this through Article 57(1)(g) and the broader cooperation mechanisms embedded in Articles 60–62, enabling coordinated enforcement and mutual assistance. This reflects the shift toward networked collaborative regulatory governance.

Stakeholder Engagement

Supervisory authorities engage with a wide range of stakeholders, including industry actors, civil society, and the general public, to ensure that regulatory approaches are informed and inclusive.

While not always framed as a standalone function, the GDPR incorporates this through consultation requirements and advisory processes under Article 57(1)(c) and (e). This supports a participatory model of regulation that enhances legitimacy and effectiveness.

Accountability and Reporting

Supervisory authorities are expected to operate transparently and remain accountable to democratic institutions. This typically involves reporting on activities, enforcement actions, and emerging systemic risks, with such reports made publicly available and accessible to relevant stakeholder groups.

Under the GDPR, Article 59 requires supervisory authorities to produce annual reports for national parliaments, thereby reinforcing institutional accountability. It also mandates that these reports be made available to the public, as well as to the European Commission and the European Data Protection Board.

These requirements position transparency not merely as a procedural obligation, but as a core mechanism for building public trust, enabling oversight, and demonstrating the effective exercise of regulatory authority.

Conclusion

The conditions of effective supervisory authorities contemplate a set of foundational institutional safeguards, including clear and merit-based appointment processes, adequate tenure and security of tenure to protect against arbitrary removal, and requirements for professional expertise. These are reinforced by obligations of confidentiality, which support the integrity of regulatory functions, and, critically, by guarantees of independence – both legal and operational, coupled with access to sufficient financial, human, and technical resources.

Across the functional capabilities, supervisory authorities emerge as integrated governance institutions, combining enforcement, advisory, educational, and strategic oversight roles. Mature regimes, such as those reflected in the GDPR, provide a well-articulated model that embeds these conditions within a coherent legal framework, balancing independence with accountability.

Taken together, the alignment of robust legal safeguards with enabling operational conditions and strong regulatory capabilities underpins the effectiveness of mature supervisory authorities. Such frameworks support the consistent protection of individual rights, and trusted data flows and trade, while fostering accountability.

Regional DPA Legislative Frameworks

The section comparatively examines the legislative provisions of the 14 Caribbean jurisdictions' respective national supervising authorities to understand their functional capabilities and conditions viewed as necessary for effective operations. The analysis reveals a consistent pattern. While many have adopted the form of modern data protection authorities, fewer have fully embedded the structural guarantees required for effective and credible oversight. See Tables 4 and 5.

Institutional Conditions

Tenure and Security of Tenure

The analysis reveals significant inconsistency across the region. Jurisdictions such as Bermuda, Jamaica, Trinidad and Tobago, and Saint Lucia demonstrate closer alignment by providing fixed terms (typically 5–7 years) and limiting removal to defined grounds such as incapacity or misconduct. These provisions reflect good international practice by insulating officeholders from arbitrary dismissal and protecting them from political interference.

However, several jurisdictions, including Barbados and Grenada, either omit tenure provisions entirely from the primary legislation or provide only vague guidance. Such omission can create institutional fragility, as officeholders may be vulnerable to informal pressure or premature removal. Under GDPR-aligned expectations, such ambiguity falls short of the requirement for structurally guaranteed independence and undermines the long-term stability of the authority.

Nature of Appointment

Given that the method of appointment is an important structural safeguard for independence, mature regimes emphasise transparent, pluralistic and multi-actor processes. These typically involve participation beyond the executive, such as consultation with opposition figures or independent bodies, to mitigate the risk of political influence and reinforce institutional legitimacy. In this regard, jurisdictions such as Bermuda and Grenada demonstrate degrees of alignment by requiring consultation between government and opposition figures, thereby diffusing appointment power. Similarly, Jamaica incorporates consultation mechanisms that strengthen both the credibility and perceived neutrality of the office.

By contrast, appointment processes that are executive-dominated or insufficiently specified fall short of good practice. Concentration of appointment power risks undermining both actual and perceived independence, as the supervisory authority may be viewed as an extension of the executive. Accordingly, the baseline requirements articulated under Article 53 should be understood as a minimum standard. Effective alignment requires that appointment frameworks be designed to institutionalise independence, ensuring that it is embedded not only in the supervising authority's formal mandate but also in the processes through which its leadership is constituted.

Qualifications, Expertise, and Professional Competence

The comparative analysis reveals a clear divide between jurisdictions that explicitly prescribe professional expertise and those that do not. Jurisdictions such as Trinidad and Tobago and Belize require qualifications spanning law, ICT, finance, and governance, reflecting closer alignment with the demands of the contemporary regulatory environment. Grenada similarly adopts a broad, multidisciplinary competency framework, reinforcing the expectation that supervisory authorities must be equipped to address complex data protection challenges.

By contrast, systems that rely on general discretion or lack specificity in qualification criteria may operate effectively in practice, but this approach carries inherent risks. The absence of codified requirements can lead to inconsistency in leadership quality and weaken institutional credibility over time. In mature regimes, expertise is not left to discretion but is formally embedded as a statutory requirement, ensuring both competence and confidence in the authority's decision-making.

Duty of Confidentiality and Professional Secrecy

Confidentiality obligations are generally well developed across the region and represent one of the stronger areas of convergence with GDPR standards. Jurisdictions such as Barbados, Belize, and Trinidad and Tobago provide clear statutory duties of confidentiality, often reinforced by oath-taking requirements or explicit prohibitions on disclosure.

However, the level of detail varies, with some jurisdictions relying on implicit obligations or general public service rules. Weaker or less explicit confidentiality provisions may not provide sufficient assurance, particularly in cases involving sensitive personal data (e.g., health records, financial information, or biometric data). Where the legal framework does not clearly define the scope, duration, and enforceability of professional secrecy obligations, there is a risk that individuals and organisations may, for example, question whether information disclosed during investigations will be adequately protected.

Accordingly, ambiguity in this area can directly undermine regulatory effectiveness and public trust, both of which are essential to the credibility of a supervisory authority.

Independence

The comparative findings reveal uneven and often incomplete implementation of this principle. Strong alignment is evident in jurisdictions such as Bermuda, Belize, the Cayman Islands, and Saint Lucia, where legislation explicitly states that the authority is not subject to direction or control.

In contrast, several jurisdictions rely on implied independence or provide no explicit guarantee. This is particularly evident in countries such as Guyana, Grenada and Saint Vincent and the Grenadines. Such approaches fall short of modern standards, which require independence to be explicit, comprehensive, and operationally effective. Importantly, independence is not limited to formal declarations; it must be reinforced through appointment processes,

tenure protections, and financial autonomy. Where these supporting structures are weak, formal independence provisions may have limited practical effect.

Resource Capability

The comparative analysis highlights this as a systemic weakness across the region. Jurisdictions such as the Cayman Islands, Bermuda, Trinidad and Tobago, and Saint Lucia demonstrate stronger frameworks, with provisions for staffing, funding mechanisms, and in some cases, independent budgetary arrangements. However, many jurisdictions rely on general public service structures without explicit guarantees of funding or staffing autonomy. This creates a significant gap between formal independence and operational reality. An authority may be legally independent but practically constrained if it lacks control over its resources.

This challenge is not unique to the Caribbean but reflects a broader issue in emerging data protection regimes. Nonetheless, current good practice standards suggest that resource adequacy is non-negotiable, and its absence represents a major barrier to achieving adequacy-level alignment.

Functional Capabilities of Supervisory Authorities

Caribbean supervisory authorities generally demonstrate stronger convergence in functional capabilities than in institutional conditions. This reflects a common pattern in emerging regulatory regimes, where formal rules and regulatory powers are often established early in the regulatory lifecycle, while the supporting institutional structures and governance capacity evolve more gradually over time¹². The dataset further reinforces this pattern. It shows that most jurisdictions have introduced core functional mandates such as enforcement, complaint handling, and advisory responsibilities, though to varying degrees. However, only a smaller subset has developed fully operational supervisory institutions with the staffing, systems, and independence needed to carry out these functions effectively in practice.

Compliance Monitoring, Investigation and Enforcement

Across the region, this is the most developed functional area, with most jurisdictions providing powers to monitor compliance, conduct investigations, and issue enforcement measures. Jurisdictions such as Barbados, Belize, Cayman Islands, and Trinidad and Tobago demonstrate strong alignment with GDPR expectations by including audit powers, inspections, and enforcement actions.

However, the level of detail in enforcement frameworks varies. Some jurisdictions set out clear sanctioning mechanisms, such as defined fines, corrective orders, and progressive enforcement measures, while others rely on broad or loosely defined powers. For example, Bermuda provides for monitoring and the issuance of warnings. However, in systems where sanction tiers are not clearly articulated, the ability to deter non-compliance may be

¹² See for example, Howlett, M., & Newman, J. (2013). After "the regulatory moment" in comparative regulatory studies: Modeling the early stages of regulatory life cycles. *Journal of Comparative Policy Analysis: Research and Practice*, 15(2), 107-121

weakened. This may result in regulators struggling to apply sanctions consistently or convincingly, reducing both regulatory impact and credibility.

Complaints Handling and Redress

Most jurisdictions, including Barbados, Belize, BVI, Saint Lucia, and Trinidad and Tobago, explicitly provide for complaint investigation and resolution mechanisms, reflecting strong alignment with international standards.

Nevertheless, gaps remain. In jurisdictions such as Antigua and Barbuda, the absence of clear complaint-handling provisions weakens access to remedies. Even where complaint mechanisms exist, the lack of explicit redress pathways or compensation frameworks in some jurisdictions may limit their effectiveness. This creates a disconnect between formal rights and practical enforcement, undermining the credibility of the regime.

Advisory Function

Most jurisdictions recognise the importance of advisory functions, aligning with GDPR Article 57, which mandates that supervisory authorities advise governments and stakeholders on data protection matters. Strong examples include Belize, Grenada, and Saint Lucia, where authorities are empowered to issue guidance, recommendations, and codes of practice.

However, in several jurisdictions, the advisory role is present but more limited or indirectly framed. Where advisory functions are narrow or implicit, authorities may struggle to act proactively or shape regulatory environments. GDPR-aligned authorities are expected not only to respond to issues but to anticipate and guide policy development, a role that is still evolving in parts of the region.

Public Awareness and Education

Many jurisdictions, including Barbados, Belize, and Saint Vincent and the Grenadines, include explicit mandates for public education and outreach. However, this function is not uniformly embedded. In jurisdictions such as The Bahamas and Antigua and Barbuda, the absence of explicit awareness provisions may hinder the development of a culture of compliance. Without sustained public engagement, individuals may remain unaware of their rights, and organisations may lack guidance on their obligations. Over time, this weakens both enforcement and trust in the regulatory framework.

Legislative and Policy Review

Jurisdictions such as Barbados, Belize, and Grenada demonstrate maturity in this area by explicitly mandating legislative review and policy input functions.

By contrast, jurisdictions such as Jamaica and Trinidad and Tobago rely more on general advisory powers without clearly defined legislative review mandates. This limits the authority's ability to act as a "policy guardian", ensuring that privacy

considerations are embedded in new laws and regulatory initiatives. Under GDPR expectations, this proactive role is essential for maintaining coherence and preventing regulatory gaps.

Research and Technology Monitoring

The ability to monitor technological developments and emerging risks is increasingly critical in modern data protection. While jurisdictions such as Barbados, Belize and BVI explicitly include research and monitoring functions, others, such as the Cayman Islands and Jamaica, rely on implicit or incidental powers.

This represents a notable gap in future-proofing regulatory capacity. Without explicit mandates, authorities may lack the institutional focus or resources to address emerging challenges such as AI, big data, and cross-border digital services. Modern and GDPR-aligned regimes treat research and monitoring as core functions, enabling authorities to remain adaptive and forward-looking.

Cooperation (Domestic and International)

Jurisdictions such as Bermuda, Cayman Islands, and Trinidad and Tobago include provisions for both domestic and international cooperation, reflecting alignment with global good practice. These frameworks enable supervisory authorities to address cross-border issues more effectively, particularly in managing data flows that extend beyond national jurisdictions.

However, several jurisdictions lack explicit or robust cooperation frameworks, particularly for international engagement. In such cases, cooperation is likely treated as incidental to the broader functions of the authority rather than as a clearly defined institutional mandate. However, weaker provisions may limit the ability to participate in cross-border enforcement or regulatory networks. This is a critical limitation for small, open economies where data flows are inherently international. Notably, under the GDPR, cooperation is essential not only for enforcement but also for achieving adequacy recognition.

Stakeholder Engagement

Modern regulatory approaches emphasise co-regulation and stakeholder engagement, including consultation, codes of practice, and collaboration with industry and civil society. Jurisdictions such as Barbados, Belize, and the Cayman Islands provide structured mechanisms for engagement, including public consultations and guidance frameworks.

In contrast, several jurisdictions rely on more implicit or informal engagement mechanisms. While functional, this limits the development of institutionalised dialogue and reduces opportunities for collaborative compliance. Notably, mature supervisory authorities embed engagement as a continuous and structured process rather than an ad hoc activity.

Accountability and Reporting

Jurisdictions such as Barbados, Bermuda, Jamaica, and Trinidad and Tobago meet current accountability standards by requiring annual reports and formal oversight mechanisms. Jamaica goes a step further by establishing a data protection oversight committee tasked with holding the Information Commissioner accountable to the public for the performance of its functions.

However, gaps remain in jurisdictions like Grenada and Saint Lucia, where reporting obligations are weak or absent. In some cases, reporting lines are directed to ministers rather than legislatures, which may compromise independence. Such accountability frameworks are likely to reduce transparency and democratic oversight, even where other elements of independence are present.

Conclusion

The analysis reveals a patterned and structured divergence from GDPR benchmarks that can be understood through two interrelated dimensions: institutional conditions and functional capability. Overall, Caribbean supervisory authorities demonstrate partial alignment with certain modern standards espoused under the GDPR, with clear areas of strength in functional capabilities alongside persistent structural and operational gaps (Table 5, Table 6).

From an institutional perspective, performance is uneven. Stronger alignment is evident in areas such as confidentiality safeguards and, to a growing extent, professional competence frameworks, where several jurisdictions have begun to embed multidisciplinary requirements. These developments indicate an emerging recognition of the technical and legal complexity of modern data governance.

However, these gains are offset by more fundamental weaknesses in tenure security, appointment processes, institutional independence, and resource autonomy. In several cases, these safeguards are either insufficiently defined or lack operational depth, limiting their effectiveness in practice. The central issue becomes less about the absence of legislative frameworks and more about the incomplete institutionalisation of the safeguards required to make those frameworks operationally effective. Mature regimes demonstrate that, in line with the GDPR, supervisory effectiveness depends on the interaction between legal authority and structural integrity. Without robust institutional design, even well-drafted statutory powers may not translate into meaningful regulatory independence or credibility.

From a functional perspective, Caribbean jurisdictions exhibit a relatively high degree of convergence with GDPR standards, particularly in relation to enforcement powers and complaints handling, which are widely present across the region. These functions form the operational core of most supervisory authorities and indicate a broadly shared understanding of basic regulatory responsibilities.

However, beyond these core functions, there is greater variability in both depth and institutionalisation. Advisory roles, research and technology monitoring, and cooperation mechanisms are inconsistently developed, with some jurisdictions providing only implicit or limited mandates. This unevenness suggests that while foundational regulatory tools are in place, advanced supervisory functions remain underdeveloped in many regimes.

A main takeaway is that although most jurisdictions have adopted the basic functional toolkit of modern data protection authorities, fewer have fully operationalised the proactive, anticipatory, and collaborative roles associated with mature GDPR-aligned regimes. Strengthening these dimensions will be essential to ensuring that supervisory authorities evolve beyond reactive enforcement bodies into strategic regulators capable of shaping data governance in increasingly complex digital environments. Jurisdictions such as the Bahamas have taken steps in this direction, with a new data protection bill aimed at aligning with current international standards and good practices, and which is now undergoing public consultation.

Table 5: Regional Supervisory Authorities: Dimensional Summary of Alignment with Modern Legal Standards

Jurisdiction	Institutional Conditions	Functional Capabilities
Antigua & Barbuda	●	●
Bahamas	●	●
Barbados	●	●
Belize	●	●
Bermuda	●	●
BVI	●	●
Cayman Islands	●	●
Grenada	●	●
Guyana	●	●
Jamaica	●	●
St Kitts & Nevis	●	●
St Lucia	●	●
St Vincent & the Grenadines	●	●
Trinidad & Tobago	●	●

Legend

● High alignment | ● Partial alignment | ● Low alignment

Table 6: Comparative Assessment of Legislative Frameworks to Support DPAs

														
Dimension	Antigua	Bahamas	Barbados	Belize	Bermuda	BVI	Cayman	Grenada	Guyana	Jamaica	St Kitts & Nevis	St Lucia	St Vincent & the Grenadines	Trinidad & Tobago
1. Tenure & Security	●	●	●	●	●	●	●	●	●	●	●	●	●	●
2. Nature of Appointment	●	●	●	●	●	●	●	●	●	●	●	●	●	●
3. Qualifications & Competence	●	●	●	●	●	●	●	●	●	●	●	●	●	●
4. Confidentiality	●	●	●	●	●	●	●	●	●	●	●	●	●	●
5. Independence	●	●	●	●	●	●	●	●	●	●	●	●	●	●
6. Resource Capability	●	●	●	●	●	●	●	●	●	●	●	●	●	●
7. Enforcement & Investigation	●	●	●	●	●	●	●	●	●	●	●	●	●	●
8. Complaints & Redress	●	●	●	●	●	●	●	●	●	●	●	●	●	●
9. Advisory Function	●	●	●	●	●	●	●	●	●	●	●	●	●	●
10. Public Awareness & Education	●	●	●	●	●	●	●	●	●	●	●	●	●	●
11. Legislative & Policy Review	●	●	●	●	●	●	●	●	●	●	●	●	●	●
12. Research & Tech Monitoring	●	●	●	●	●	●	●	●	●	●	●	●	●	●
13. Cooperation	●	●	●	●	●	●	●	●	●	●	●	●	●	●
14. Stakeholder Engagement	●	●	●	●	●	●	●	●	●	●	●	●	●	●
15. Accountability & Reporting	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Legend

- = explicit provision with elements of modern/GDPR-equivalence, at minimum
- = partial/implied provision
- = no clear statutory provision

A Legislative and Operational Maturity Model for Supervisory Authorities

To continue the assessment of the development of supervisory authorities across jurisdictions, a legislative and operational maturity model is introduced. This model provides a structured and cogent way to evaluate how closely national frameworks align with current good practice standards, such as the GDPR.

This model recognises that jurisdictions do not move from absence to full compliance in a single step. Instead, they progress through distinct stages of institutional and functional development, moving from basic or fragmented arrangements toward fully independent, well-resourced, and proactive regulatory authorities to meet the evolving and complex digital ecosystem, comparable to mature regimes.

The five-tier model, ranging from the lowest to the highest levels of maturity, reflects the following stages (Figure 4):

- Pre-Established (Tier 5)
- Establishing (Tier 4)
- Operating (Tier 3)
- Evolving (Tier 2), and
- Maturing (Tier 1)

It captures the progression of development and growth, focusing on the legislative cycle, Institutional conditions (including independence, tenure, resources, etc), and Functional capabilities (including enforcement, advisory, cooperation, etc).

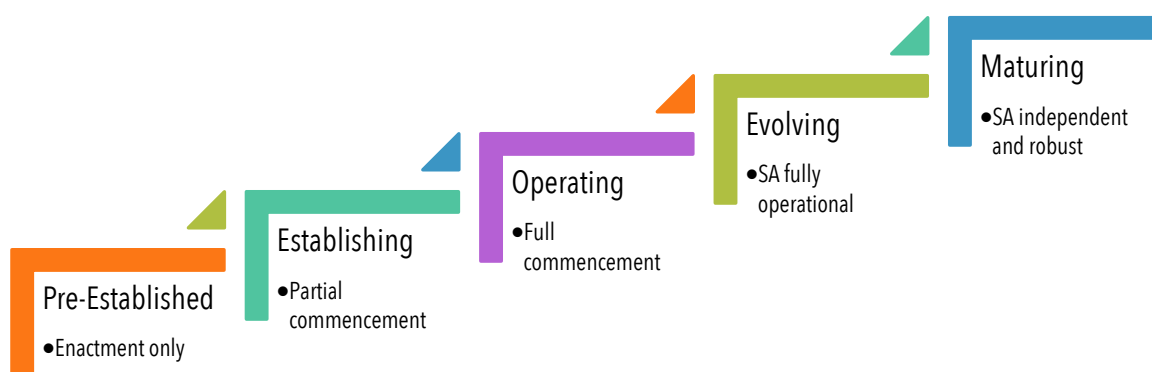


Figure 4: Legislative and Operational Maturity Model

Tier 5: Pre-Established

At this tier, a data protection law exists, and a supervisory authority is legally created, but the law (or key provisions establishing the authority's powers/functions) has not yet come into force, or implementation has not begun.

This is the formal legislative stage without operational reality.

Key Characteristics:

- The law has been enacted by Parliament/legislature
- Commencement is delayed or suspended
- Supervisory authority may exist only in legislative provisions
- No operational staff, budget, or enforcement activity
- No exercised powers (investigation, complaints, sanctions)
- Good practice alignment is purely formal

At this stage, the system is non-operational in practice, even if structurally aligned legislatively. Countries such as Saint Kitts, Saint Lucia, Grenada, Belize and Guyana currently fall in this tier (Figure 5).

Transition to the next tier requires, at a minimum, commencement of the framework in whole or in part.

Tier 4: Establishing

The data protection law has commenced, in part, and the supervisory authority is legally active, but institutional and functional development is still only partial or uneven.

This stage reflects initial legal activation, where the framework is live but incomplete.

Key Characteristics:

- Supervisory authority is legally active under the commencement provisions
- Some functions are operational (e.g., public awareness, complaints intake or advisory role)
- Partial staffing and administrative setup (e.g., the Commissioner has been appointed)
- Independence may be declared but not fully secured
- Resource allocation may be transitional or ministry-dependent
- Enforcement powers exist, but may be limited in practice

This stage corresponds to early implementation reality, where normative legislative structures exist, but:

- Operational capacity is absent or inconsistent
- Institutional safeguards are still forming
- The regulatory impact remains limited

Countries such as Barbados and Jamaica currently reflect this reality (Figure 5).

Transition to the next tier requires at least full operationalisation of the legislative framework.

Tier 3: Operating

The data protection law is fully commenced, and the supervisory authority is actively functioning across its core mandate, with measurable institutional and regulatory activity.

This is the core functional stage where the authority is operational in practice.

Key Characteristics:

- Full commencement of legislation
- Active enforcement, investigation, and complaint-handling functions
- Operational staffing and administrative systems in place
- Defined but variable independence safeguards (legal and practical)
- Budget exists, though it may not be fully autonomous
- Advisory, awareness, and cooperation functions are active (to varying degrees)

Authorities at this stage are functionally comparable to working DPAs, but may still fall short of full maturity due to:

- incomplete independence
- limited resource autonomy
- uneven institutional robustness

Countries such as the Cayman Islands and Bermuda fall within this tier (Figure 5).

Transition to the next tier levels may require a combination of legal reform and operational design and development to bridge institutional conditions and functional capabilities.

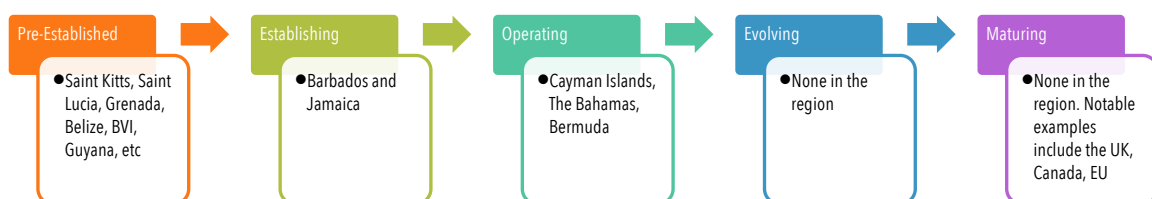


Figure 5: Regional Maturity Mapping

Tier 2: Evolving

The authority is fully operational and increasingly aligned with current good practices and standards, but is still strengthening governance, autonomy, and advanced regulatory functions. At this stage, countries may also recognise the need for law reform to achieve tier 1 status.

This stage reflects advanced operational maturity with ongoing institutional consolidation.

Key Characteristics:

- Strong enforcement and investigative capacity
- Increasingly robust independence safeguards
- More formalised appointment and tenure protections
- Dedicated or semi-autonomous funding arrangements
- Expanded advisory, policy, and research roles
- Active domestic and international cooperation
- Structured stakeholder engagement mechanisms

Authorities here are approaching GDPR adequacy readiness, but still refining:

- full budgetary independence
- complete insulation from executive influence
- advanced supervisory cooperation mechanisms

No jurisdiction in the current dataset fits this profile.

Tier 1: Maturing

At this level, the supervisory authority is fully operational, structurally independent, and institutionally robust, reflecting the core institutional conditions and functional capabilities, such as the requirements articulated in Articles 52–59 of the GDPR, and highlighted in the previous section.

This is the highest level of legislative and operational maturity, representing near-full alignment with GDPR supervisory authority expectations.

Key Characteristics:

- Full legal and operational independence
- Transparent, multi-stakeholder appointment systems
- Secure tenure and strict removal safeguards
- Full budgetary and staffing autonomy
- Comprehensive functional mandate
- Strong accountability via parliamentary reporting
- Institutionalised stakeholder engagement and transparency

This stage reflects GDPR adequacy-ready supervisory authorities, capable of:

- independent decision-making
- cross-border regulatory cooperation
- proactive governance of digital ecosystems

No jurisdiction in the current dataset fits this profile. Jurisdictions such as the UK, Ireland, Canada and the EU are notable examples.

Conclusion

This legislative and operational maturity model introduces a critical distinction often overlooked in traditional maturity frameworks: legal existence does not equate to operational maturity. It reframes institutional development as a progression through three essential transitions:

- Enactment (Pre-Established stage)
- Commencement (Establishing stage), and
- Full operationalisation (Operating, Evolving, and Maturing stages)

By embedding global good practice standards, such as the GDPR, directly into its structure, the model ensures both legal and functional coherence. It emphasises independence and sound governance design, addresses the necessity of adequate resources and institutional infrastructure, defines clear functional authority and enforcement capacity, and reinforces robust accountability and transparency mechanisms

In doing so, the model underscores the urgent need for structured, practical guidance in establishing supervisory authorities, not only within the region but across other emerging jurisdictions seeking to progress beyond formal legal establishments toward effective regulatory performance.

Policy Recommendations

Building on the analysis of legislative frameworks, institutional conditions, and operational realities across the Caribbean, this section sets out a structured set of policy, legal, and institutional recommendations to strengthen data protection governance in the region. The findings of this report highlight a clear and consistent challenge, which is that while many jurisdictions have adopted modern data protection laws aligned with international benchmarks such as the GDPR, the effectiveness of these frameworks is constrained by gaps in implementation, particularly in relation to supervisory authorities.

In this context, the recommendations are designed to support a strategic shift from legislative adoption to operational effectiveness, with a focus on enhancing the independence, capacity, and functionality of supervisory authorities. They are tailored to the varying levels of maturity across jurisdictions and directed toward key stakeholders, including governments, legislatures, regulators, regional organisations, and development partners. Collectively, these measures aim to bridge the gap between law and practice, strengthen regulatory credibility, and support the Caribbean's deeper integration into the global data governance ecosystem.

Strategic Policy Direction

1. Shift from Legal Adoption to Operational Readiness

Governments should prioritise the implementation and operationalisation of existing data protection laws. This includes:

- Establishing supervisory authorities where they do not yet exist
- Ensuring authorities are fully staffed, funded, and functional
- Sequencing reforms to prioritise enforcement capacity over further legislative expansion

2. Adopt a Phased Maturity Approach

Using the report's maturity model, jurisdictions should pursue tiered reform strategies that reflect their current positioning at largely nascent and transitional stages. Prioritising pragmatic, resource-efficient approaches will help accelerate progress while ensuring reforms remain realistic and sustainable:

- Tier 4–5 jurisdictions: legal commencement and institutional establishment
- Tier 3 jurisdictions: strengthening independence and enforcement capability

At the same time, lower-tier jurisdictions should prioritise engagement at the international and regional levels, including strengthened cooperation mechanisms, while progressively advancing targeted regulatory enhancements in line with their institutional capacity.

Enhance Legal and Regulatory Frameworks

1. Strengthen Statutory Guarantees of Independence

Legislation should be amended, where necessary, to:

- Provide clear tenure protections and limit arbitrary removal
- Establish transparent, merit-based appointment processes
- Insulate supervisory authorities from political or executive direction

These measures are essential to align with international standards reflected in the GDPR and global best practice.

2. Clarify and Expand Enforcement Powers

Legal frameworks should ensure supervisory authorities have:

- Explicit powers to investigate, audit, and compel information
- Authority to issue binding decisions, sanctions, and administrative penalties
- Clear procedures for appeals and judicial review

Where powers exist but are fragmented, consolidation into a coherent enforcement framework is recommended.

3. Codify Accountability and Reporting Obligations

To strengthen transparency and oversight:

- Supervisory authorities should be required to submit annual reports to Parliament and certain activity reports publicly
- Financial and operational reporting obligations should be clearly defined
- Mechanisms for public disclosure of decisions and enforcement actions should be introduced

4. Strengthen Legal Provisions for Cooperation

Legislation should explicitly provide for:

- Cross-border cooperation with foreign supervisory authorities
- Participation in regional and international data protection networks
- Recognition of adequate jurisdictions and safeguards for data transfers

Prioritise Institutional Strengthening

1. Ensure Adequate and Sustainable Resourcing

Governments should:

- Allocate dedicated budget lines for supervisory authorities
- Support recruitment of technical, legal, and investigative expertise
- Explore cost-recovery mechanisms (e.g., fees, administrative penalties) where appropriate

Resource adequacy is a prerequisite for effective enforcement.

2. Build Technical and Operational Capacity

Supervisory authorities should invest in:

- Training in multi-disciplinary areas, including cybersecurity and data governance
- Development of standard operating procedures (SOPs) for registration, investigations and complaints handling
- Adoption of case management and regulatory technology tools

3. Strengthen Internal Governance Structures

Supervisory Authorities should establish:

- Clear organisational structures with defined roles and responsibilities
- Internal accountability mechanisms, including audit and compliance functions
- Codes of conduct and ethics frameworks for staff

Foster Functional Effectiveness

1. Enhance Enforcement and Compliance Strategies

Supervisory authorities should adopt a risk-based regulatory approach, including:

- Proactive audits of high-risk sectors
- Use of graduated enforcement tools (warnings, fines, directives)
- Development of compliance frameworks for both public and private sectors

2. Improve Complaints Handling and Redress Mechanisms

To increase accessibility and trust:

- Establish clear, user-friendly complaint procedures
- Implement timelines for complaint resolution
- Provide alternative dispute resolution mechanisms, including mediation

3. Expand Advisory and Guidance Functions

Authorities should:

- Issue guidelines, codes of practice, and sector-specific guidance
- Provide advisory opinions on emerging technologies and data use cases
- Engage proactively with policymakers on legislative reforms

4. Strengthen Public Awareness and Education

Governments and supervisory authorities should:

- Develop national awareness campaigns on data protection rights and obligations

- Integrate data protection into digital literacy and education programmes
- Engage with businesses, civil society, and public institutions

Encourage Regional Cooperation and Integration

1. Promote Regional Harmonisation

Regional organisations and governments should:

- Work toward greater alignment of legal frameworks and regulatory standards
- Develop model laws, guidelines, and shared regulatory tools
- Facilitate peer learning and exchange of best practices

2. Establish Regional Support Mechanisms

Consideration should be given to:

- Creating regional centres of excellence for data protection
- Pooling technical expertise across jurisdictions
- Supporting smaller states through shared services or joint regulatory initiatives

3. Strengthen Engagement with International Partners

Development partners and international organisations can support:

- Capacity building and technical assistance
- Funding for institutional development
- Benchmarking and peer review exercises

Nurture Stakeholder Engagement

1. Encourage Industry Compliance and Accountability

Businesses should be supported to:

- Implement data protection compliance programmes
- Appoint data protection officers where appropriate
- Adopt privacy-by-design and accountability practices

2. Foster Multi-Stakeholder Engagement

Supervisory authorities should:

- Engage with civil society, academia, and industry stakeholders
- Encourage the development of codes of conduct and certification schemes
- Facilitate consultation processes for policy and regulatory development

The recommendations reflect a central finding of this report that effective data protection requires more than legislation; it requires institutions that can act and do so effectively. Strengthening supervisory authorities across the Caribbean will be critical to translating legal frameworks into meaningful regulatory outcomes, fostering trust, enabling digital transformation, and positioning the region within the evolving global data governance ecosystem.

Implementation Priorities

To maximise impact, countries should prioritise the following actions, with the flexibility to advance through short-, medium-, and long-term goals according to their level of maturity and readiness:

Short-term (0–2 years):

- Operationalise supervisory authorities
- Secure funding and staffing
- Establish basic registration, enforcement and complaints mechanisms
- Leverage cooperation, especially at the domestic and regional levels

Medium-term (2–5 years):

- Strengthen independence and accountability frameworks
- Expand enforcement capabilities and technical expertise
- Enhance public awareness and stakeholder engagement

Long-term (5+ years):

- Achieve full regulatory maturity
- Deepen international cooperation and adequacy alignment
- Integrate advanced regulatory tools and innovation frameworks

Conclusion

This report has examined the evolution of data protection frameworks across the Caribbean, with a particular focus on the role, design, and effectiveness of supervisory authorities. It demonstrates that while the region has made meaningful progress in aligning its legislative frameworks with international standards, most notably those reflected in the GDPR, a critical gap persists between formal legal adoption and practical regulatory effectiveness.

At the centre of this gap lies the operational reality of supervisory authorities. The analysis confirms that the existence of a data protection law, even where closely aligned with global best practice, does not in itself ensure effective oversight. Rather, outcomes are determined by the extent to which supervisory authorities are independent, adequately resourced, technically capable, and empowered to act. Where these conditions are absent or only partially realised, regulatory systems remain constrained, and the objectives of data protection, namely, accountability, trust, and enforcement, are only weakly achieved.

The findings further highlight that institutional conditions and functional capabilities are mutually reinforcing. Strong enforcement powers, complaints mechanisms, and advisory functions are essential, but their effectiveness depends on the institutional environment within which they operate. Weaknesses in appointment processes, tenure protections, or resource allocation can significantly undermine even well-designed statutory mandates. Conversely, jurisdictions that have combined robust institutional safeguards with comprehensive functional powers demonstrate the highest levels of regulatory maturity and alignment with international standards.

The introduction of our legislative and operational maturity model provides a structured lens through which to understand these differences. It reveals a region characterised by uneven progress: none has yet achieved top-tier status, while many remain in transitional stages, where legal frameworks exist but implementation is partial or incomplete. This limitation has important implications for regulatory credibility, cross-border data flows, and the region's ability to participate effectively in the global digital economy.

The evidence also underscores a broader and more structural insight: data protection reform is not solely a legislative exercise, but an institutional one. The experience of earlier regional initiatives, as well as the current wave of GDPR-inspired reforms, illustrates that without sustained investment in institutional capacity, legal modernisation risks outpacing implementation. This challenge is particularly pronounced in small states, where resource constraints and competing policy priorities can limit the speed and depth of institutional development.

Looking ahead, the pathway to effective data governance in the Caribbean requires a deliberate shift in focus from the enactment of laws to the operationalisation of supervisory authorities. This entails strengthening legal guarantees of independence, ensuring transparent and merit-based appointment processes, securing sustainable funding and technical expertise, and embedding accountability through reporting and oversight mechanisms. It also requires greater emphasis on regional cooperation, knowledge-sharing, and the development of practical tools to support implementation.

Ultimately, the credibility and effectiveness of Caribbean data protection regimes will be judged not by the sophistication of their legislative texts, but by the ability of their institutions to enforce the law, uphold rights, and respond to an increasingly complex digital environment. Bridging the gap between law and practice is therefore not simply a technical objective; it is a strategic imperative for building trust, enabling innovation, and positioning the region within the evolving architecture of global data governance.

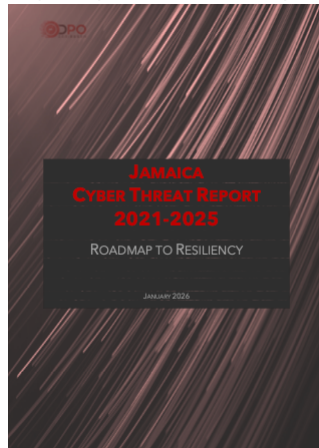
In this regard, strengthening supervisory authorities represents both the central challenge and the most immediate opportunity for advancing data protection in the Caribbean.

DPO Caribbean Publications

Jamaica Cyber Threat Report 2021-2025

ISBN 978 976 97440 2 8

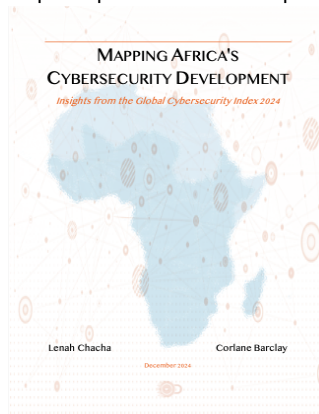
<https://dpocaribbean.com/publications>



Mapping Africa's Cybersecurity Development: Insights from the Global Cybersecurity Index 2024

ISBN 978 976 97440 1 1

<https://dpocaribbean.com/publications>



An Analysis of the Global Cybersecurity Index (GCI) 2024: Progress, Challenges and Opportunities for Cybersecurity in the Caribbean

ISBN 978 976 97440 0 4

<https://dpocaribbean.com/publications>





From Laws to Practice

Strengthening Data Protection Authorities in the Caribbean

DPO Caribbean

<https://dpocaribbean.com/>
20 West Kings House Road
Kingston, Jamaica, WI

ISBN 978 976 97440 3 5

Published in Kingston
Jamaica, WI, 2026