Harmonising Data Protection Legislation across the Commonwealth Caribbean

Can the Commonwealth Model Provisions on Data Protection ("CMP") drive harmonisation of the collection and retention of Data throughout the Commonwealth Caribbean?

Justine A. Collins[1]

Introduction

The question of whether data privacy can be harmonised throughout the Commonwealth, based on the Commonwealth Model Provisions ("CMP") on Data Protection is predicated on two presumptions: i) that the passing of a comprehensive data protection law will lead to its implementation and ii) that such implementation will produce the harmonization and consequently protected data flows throughout the Commonwealth.

While the CMP is sufficiently comprehensive and has detailed guidance on the comparisons with international instruments on data protection, such as General Data Protection Regulation in the European Union ("GDPR"), Organisation for Economic Co-operation and Development ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Asia -Pacific Economic Cooperation ("APEC") Privacy Framework and Association of Southeast Asian Nations ("ASEAN") Framework on Personal Data Protection, it is not sufficient to harmonise the collection and retention of personal data throughout the Commonwealth. The CMP is relatively current and has successfully provided a comprehensive model law which can be replicated. However, the alignment of national law to the CMP will not necessarily lead to harmonisation. Many Commonwealth Caribbean states, for example, have passed data protection laws, yet few states have fully implemented the data protection laws, and introduced enforcement actions to sufficiently deter data controllers from breaching the data protection laws.

This note examines the importance of trans-border flows in driving harmonisation of data protection law efforts within the Commonwealth Caribbean. It analyses key differences between the Jamaican Data Protection Act and the Commonwealth Model Provisions, as well as the importance of alignment in cross-border provisions. Ultimately it concludes that the Commonwealth Caribbean region has fairly comprehensive data protection laws, and most countries have passed or are in the process of passing laws surrounding data protection. However, challenges in implementation of the data protection laws and adequacy decisions across the region stymie the intended effect of the passage of the data protection laws.

---

[1] Justine A. Collins, CIPP/E, CIPM, FIP, AIGP is a Partner at Hart Muirhead Fatta, Attorneys at Law, in Jamaica

Comparison between Commonwealth Model Provisions on Data Protection and Jamaican Data Protection Act

The CMP is commendable in the way it aligns and simplifies key concepts across OECD Guidelines, GDPR, APEC and ASEAN frameworks and provides commentary to assist jurisdictions in determining what works best for their local realities.

The CMP also integrates principles derived from the Fair Information Practice Principles (FIPPS), such as lawfulness, fairness, transparency, purpose limitation, providing greater alignment with best practices.

The commentary simplifies complex jargon in a manner which is accessible. Most provisions appear to align with the GDPR, which the Jamaican Data Protection Act ("JDPA") closely resembles. The JDPA and CMP align closely due to their references to the GDPR.

Data subjects

However, there are divergences in key concepts from the JDPA. The definition of "data subject under the CMP includes a natural and a legal person. The JDPA only permits a natural person to be categorised as a data subject. In the commentary, the CMP contemplates that "*legal persons may be harmed by information and power assymetries in personal data processing and poor data governance and security practices. The extension of protection to legal persons simplifies the regulatory environment for data controllers and data processors and minimises the risk of arbitrary differentiation between different forms of corporate entities*"[2].

The CMP acknowledged that it is only the GDPR which left the possibility open for a legal person to be a data subject. The challenge with this suggestion is that it becomes unclear from a data governance perspective how additional safeguards in relation to data subjects who are legal persons would be treated and ultimately, how that data is categorised. Nevertheless, providing safeguards for an additional category of data subject is noteworthy.

Fairness

Additionally, the principle of fairness, which is provided under section 22 of the JDPA differs in some respects from the CMP. The JDPA states that personal data are processed fairly if persons are not misled or deceived as to the purposes of the processing at the time of collection, and that they are provided with certain information specified in section 22(6) (which typically forms the basis of data controllers' privacy notice).

[2] Commonwealth Model Provisions on Data Protection: Commentary and International Comparison Part II

The CMP goes a bit further and requires the data controller to consider the data subject's "legitimate and reasonable expectations"[3] in the processing of the personal data. Further, the CMP states that if the processing causes an unjustified detriment to the fundamental rights and interests of the data subject, the rights and interests of a group who share significant or protected characteristics, or important objective of general or public interest, it could be deemed to be unfairly processed. The CMP provides additional guarantees of fairness through these provisions, widening the scope to include "unjustified detriment" which would require controllers to assess the proportionality of their processing activities to the rights of persons, and in particular, vulnerable groups.

This provision is one which this writer believes ought to be incorporated in data protection laws. The JDPA, like most GDPR aligned laws, contains an obligation on controllers to fairly and lawfully process personal data, but most often it gets lost in the emphasis on lawfulness of processing. The CMP Commentary recognises this and states: "*This principle recognises that even if personal data is processed lawfully on the basis of one of the legal grounds…the processing may still be considered unfair if it goes beyond what the data subject has reasonable expected…. The concept of fairness is well established, if largely undefined in international data protection instruments*."[4] This recognition is one of the key strengths of the CMP.

Data breach notification

Finally, a significant divergence is in relation to timelines for data breach notification. The JDPA and the GDPR require that the supervisory authority/regulator and data subjects who are likely to be affected by a data breach within 72 hours of becoming reasonably aware of the breach.

The CMP requires that the data breach notification to the supervisory authority is to be made within "timely manner" where reasonably likely to adversely affect individual rights. This is to reduce over notification of reports, which the CMP recognises may be a challenge for regulators. Additionally, the timeline accords with a more practical approach, as it is likely within 72 hours that all relevant investigations related to a data breach (including the nature) may not be determined within that time, and subsequent reports would need to be provided.

Likewise, the data subjects are to be notified in circumstances where it is reasonably likely to entail a "serious interference" with rights "without undue delay", reflecting a more practical approach to notification.

Essential equivalence and the issue of cross-border data flows

[3] Commonwealth Model Provisions on Data Protection: section 7(2)
[4] Commonwealth Model Provisions on Data Protection: Commentary and International Comparison s. 7(1)

International trade is a significant driver in an effort to harmonize data protection laws. Increasing interconnection and the more significant role that data plays in the global digital economy means that more countries will be motivated to align their legislative framework with international best practices.

The 2020 ruling in Schrems II[5], and consequent EU-US Data Privacy Framework in 2023 and the new standard contractual clauses demonstrate how integral cross-border data flows are important in international trade. While the concerns raised by privacy activist Schrems did not result in a federal data protection law in the US, it underscored how privacy concerns raised in Europe may influence bilateral trade agreements, while preserving EU data subjects' privacy rights.

The Schrems decision establishes the test for "essential equivalence" in determining whether a third-party country can be deemed to have an adequate level of protection with EU law. The test is not whether the third country provides "*a level of legal protection that is identical to that guaranteed in the EU, but rather, whether the third country, by its domestic law or international commitments, has a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union*".[6]

Consequent to this decision, standard contractual clauses, which are used as a contractual method to legitimise personal data transfers, were revised to ensure that data importers were adhering to "essentially equivalent" standards as the GDPR when receiving personal data from the EU. In this way, international trade can be an important facilitator for the harmonization of personal data rules, commencing with contractual arrangements between parties.

Similarly, several Commonwealth Caribbean states began data privacy initiatives for international trade reasons. The Commonwealth Caribbean states were required to pass data protection legislation pursuant to an economic partnership agreement between the Caribbean Community ("CARICOM") through CARIFORM and the EU in 2008. Many of the Commonwealth Caribbean states passed laws within the years following 2008. The table reproduced below (Table 1: Status of Commonwealth Caribbean Data Protection Laws) demonstrates the progress in the passage of these laws, except for the Commonwealth of Dominica, all the Commonwealth Caribbean states have either passed or is in the process of passing a data protection law.

In fact, the Bahamian data protection regulator in its annual report for 2012 stated that the passing of the Data Protection (Privacy of Personal Information) Act 2003 was a critical first step for the Bahamas in applying to obtain an adequacy decision from the

[5] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Judgment of the Court (Grand Chamber) of 16 July 2020.
[6] Ibid

European Commission for transborder flows. This further highlights the importance of international trade in driving the adoption of data protection laws. This legislation is broadly based on the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

Table 1: Status of Commonwealth Caribbean Data Protection Laws

Commonwealth Caribbean country	Law passed	Cross-border transfer rules	Status of implementation	Comments
Jamaica	Data Protection Act 2020	s. 31- Eighth standard	Office of Information Commissioner established, and registration of data controllers has commenced. S.1-4, Part II, s.14-20, 21(1), (3), (4) & (5), s. 22-31, Part V, s. 56- 61, 63-69, 71-77 & 2nd and 4th Schedules	Most provisions in force since 2023, with the notable exception of the enforcement provisions
Antigua & Barbuda	Data Protection Act, 2013 (No. 10 of 2013)	None	In force, new Information Commissioner appointed in 2024 after a 2-year vacancy	Policy considerations for the development of data protection and privacy legislation in the Eastern Caribbean Currency Union published in March 2025
The Bahamas	Data Protection (Privacy of Personal Information) Act 2003	s.17	Office of Data Protection Commissioner established in 2007, Act in force since 2007.	Commissioner may prohibit transfer where failure to provide protection by contract or otherwise equivalent to law
Barbados	Data Protection Act 2019	Part IV (s.22-28)	Majority of provisions in force (except sections 50, 51, 52, 55, 56 and 57), Data Protection Commissioner appointed in 2021.	Substantially aligned with GDPR in relation to adequacy decisions, appropriate safeguards and derogations
Belize	Data Protection Act 2021	Part IV (s.23-29)	Not in effect, and regulator not appointed yet	Transfer of data for cloud storage does not require consent. Still in draft

Commonwealth Caribbean country	Law passed	Cross-border transfer rules	Status of implementation	Comments
Dominica	None			Policy considerations for the development of data protection and privacy legislation in the Eastern Caribbean Currency Union published in March 2025
Grenada	Data Protection Act 2023	s.10(1)(e)	Not in effect as yet, but passed in 2023. No regulator appointed.	Policy considerations for the development of data protection and privacy legislation in the Eastern Caribbean Currency Union published in March 2025
Guyana	Data Protection Act 2023	s.23-29	Not in effect as yet, but passed in 2023. No regulator appointed.	
St. Kitts & Nevis	Data Protection Act 2018	None	Not in effect as yet, but passed in 2023. No regulator appointed, but discussions about appointment of an Information Commissioner under the Freedom of Information bill. Unclear whether the role will include both functions.	Not yet in force
St. Lucia	Data Protection Act 2011	s.45	Part 1, s. 32-43 of Part III, Part VI and para (a) to (g) of Schedule 2 in force in 2023. No appointment of Data Protection Commissioner	Exemption if transfer concerns public security
St. Vincent & Grenadines	Privacy Act, No.18 of 2003	None	Not in effect, and regulator not appointed yet	Applicable to public authorities, no evidence that it is in force

Commonwealth Caribbean country	Law passed	Cross-border transfer rules	Status of implementation	Comments
Trinidad & Tobago	Data Protection Act, Chap. 22:04 2011	s.72(1)	Part One, Sections 1 to 6, and Part Two, Sections 7 to 18, 22, 23, 25(1), 26 and 28, and Part Three, Section 42(a) and (b) of the Act have been partially proclaimed. No Information Commissioner established	Cross-border disclosure as a requirement of code of conduct requires consent. Limited application of Act- s 7 to 18, 22, 23, 25(1), 26 and 28 (2012) & s. 42(a) and (b) in 2021

As the table above demonstrates, various Commonwealth Caribbean jurisdictions passed their data protection laws after the Economic Partnership Agreement in 2008 with the EU. Following the passage of the GDPR in 2016, a number of these laws which were passed subsequently, aligned with the GDPR.

Implications of fragmented implementation across the Commonwealth Caribbean

However, many of these laws have not been fully implemented or brought into operation as yet.

The Bahamas is the only jurisdiction which has fully implemented their law and established a regulator. Other states, Jamaica, Antigua and Barbuda, and Barbados have implemented some provisions and appointed a regulator. Trinidad and Tobago, one of the earliest adopters of data protection laws in 2011, has yet to bring their legislation fully in force and has no regulator. Others, like Belize, Grenada and Guyana have not brought the law into effect yet. Dominica has not passed any data protection law. However, the oldest data protection legislation in the Caribbean, St Vincent and the Grenadines, was passed in 2003 and has yet to be brought into force or have a regulator appointed.

Several of these jurisdictions face resource challenges, particularly where some provisions have not been brought into force. The Office of the Information Commissioner ("OIC"), the data protection regulator in Jamaica, reported at its Data Privacy Conference in February 2025 that it had collaborated with jurisdictions in the Eastern Caribbean through the World Bank to highlight and assist with capacity building in implementing their data protection laws, yet, all the provisions of the Jamaican Data Protection Act have not been brought info force. Jamaica has not brought into force the enforcement provisions, which remain critical to the effectiveness of data protection laws, five years after the law was passed and three years after it was brought into force.

Other jurisdictions with older provisions, like the Bahamas who passed their law in 2003, have not seen any significant enforcement or cases emanate therefrom: "*from an enforcement and litigation standpoint, the case law in The Bahamas as it relates to data protection violations is scant.*"[7]

The phased approach in implementation is usually done to provide data controllers with sufficient time to put in place their privacy compliance programmes. Ultimately, without full implementation of the data protection rules, citizens are not able to benefit from the protections and rights it affords and compromising accountability in the event of a data breach. In 2023, there were a series of significant cyber-breaches in Trinidad & Tobago, which led to extensive discussions on the operationalisation of the Data Protection Act 2011, which was expected to be concluded by the end of 2024.[8]

Recommendations for harmonisation of data protection across jurisdictions

It is submitted that the challenge the Commonwealth Caribbean jurisdictions face is not one which the CMP can specifically address. There are sufficient international instruments on data protection which can provide guidance for the Commonwealth Caribbean jurisdictions, such as the GDPR, the OECD Guidelines and the FIPPS. The CMP provides clarity, alignment and useful commentary to assist in the interpretation of data protection concepts to add to the repository of international frameworks available.

The challenge is in the lack of full implementation across jurisdictions, particularly, the cross-border and enforcement provisions which would drive increased observation of data privacy. Once Commonwealth Caribbean jurisdictions can strengthen their regulatory bodies, and simultaneously, attempt to enable adequacy decisions for safe cross-border transfers of personal data across the region, there may be greater likelihood of harmonization.

Key considerations for determining whether a country is deemed to have an adequate level of protection for data protection under the GDPR and the CMP are whether the country has respect for human rights and fundamental freedoms, its data protection rules and enforcement, as well as their rules for onward transfers of personal data. The implementation of trans-border data rules and enforcement are crucial to harmonising data protection norms across jurisdictions. If Commonwealth Caribbean data protection regulators are empowered to institute adequacy decisions in respect of their regional partners in CARICOM, this would be an important step in facilitating regional trade.

Furthermore, public awareness by regulators and stakeholders is critical in driving implementation. As the Information Commissioner in Jamaica noted at the inaugural Data Privacy Day Conference in February 2025: "*We recognise that establishing a robust*

---

[7] **Chambers Global Practice Guides: Data Protection & Privacy**- The Bahamas: Law & Practice, Sean McWeeney Jr- Graham Thompson 2021.

[8] https://www.loopnews.com/content/data-protection-act-to-be-proclaimed-in-2024/

data protection framework is not simply about enacting legislation, but also about creating a privacy-conscious society in which individuals understand their rights and are empowered to exercise them."

By focusing on strengthening data protection regulators' capacity, as well as focusing on cross border transfers and public awareness campaigns, these may be more conductive to attempts at harmonization, rather than a focus on alignment to the CMP. The CMP has a role in being an important international instrument and reference, however, alignment with the CMP, in the absence of Commonwealth Caribbean governments fully implementing their data protection laws, would not lead to this harmonization. While the present geo-political climate may not lend itself to extensive discussions on increasing inter-connectedness, it is hoped that a focus on cross-border trade will encourage the harmonisation across jurisdictions sought to be achieved by the CMP.