United Nations
ECLAC

ECLAC SUBREGIONAL HEADQUARTERS FOR THE CARIBBEAN

FOCUS

Magazine of the Caribbean Development and Cooperation Committee (CDCC)

DATA PROTECTION IN THE CARIBBEAN

ISSUE 1 / JANUARY - MARCH 2020

ABOUT ECLAC/CDCC

The Economic Commission for Latin America and the Caribbean (ECLAC) is one of five regional commissions of the United Nations Economic and Social Council (ECOSOC). It was established in 1948 to support Latin American governments in the economic and social development of that region. Subsequently, in 1966, the Commission (ECLA, at that time) established the subregional headquarters for the Caribbean in Port of Spain to serve all countries of the insular Caribbean, as well as Belize, Guyana and Suriname, making it the largest United Nations body in the subregion.

At its sixteenth session in 1975, the Commission agreed to create the Caribbean Development and Cooperation Committee (CDCC) as a permanent subsidiary body, which would function within the ECLA structure to promote development cooperation among Caribbean countries. Secretariat services to the CDCC would be provided by the subregional headquarters for the Caribbean. Nine years later, the Commission's widened role was officially acknowledged when the Economic Commission for Latin America (ECLA) modified its title to the Economic Commission for Latin America and the Caribbean (ECLAC).

Key Areas of Activity

The ECLAC subregional headquarters for the Caribbean (ECLAC/CDCC secretariat) functions as a subregional think-tank and facilitates increased contact and cooperation among its membership. Complementing the ECLAC/CDCC work programme framework, are the broader directives issued by the United Nations General Assembly when in session, which constitute the Organisation's mandate. At present, the overarching articulation of this mandate is the Millenium Declaration, which outlines the Millenium Development Goals.

Towards meeting these objectives, the Secretariat conducts research; provides technical advice to governments, upon request; organizes intergovernmental and expert group meetings; helps to formulate and articulate a regional perspective within global forums; and introduces global concerns at the regional and subregional levels.

Areas of specialization include trade, statistics, social development, science and technology, and sustainable development, while actual operational activities extend to economic and development planning, demography, economic surveys, assessment of the socio-economic impacts of natural disasters, climate change, data collection and analysis, training, and assistance with the management of national economies.

The ECLAC subregional headquarters for the Caribbean also functions as the Secretariat for coordinating the implementation of the Programme of Action for the Sustainable Development of Small Island Developing States. The scope of ECLAC/CDCC activities is documented in the wide range of publications produced by the subregional headquarters in Port of Spain.

MEMBER COUNTRIES

Antigua and Barbuda
The Bahamas
Barbados
Belize
Cuba
Dominica
Dominican Republic
Grenada
Guyana
Haiti
Jamaica
Saint Kitts and Nevis
Saint Lucia
Saint Vincent and the Grenadines
Suriname
Trinidad and Tobago

ASSOCIATE MEMBERS:

Anguilla
Aruba
British Virgin Islands
Cayman Islands
Curaçao
Guadeloupe
Martinique
Montserrat
Puerto Rico
Sint Maarten
Turks and Caicos Islands
United States Virgin Islands

CONTENTS

FOCUS: ECLAC in the Caribbean is a publication of the Economic Commission for Latin America and the Caribbean (ECLAC) subregional headquarters for the Caribbean/Caribbean Development and Cooperation Committee (CDCC).

EDITORIAL TEAM:

Director	Diane Quarless, ECLAC
Copy Editor	Denise Balgobin, ECLAC
Coordinator	Johann Brathwaite, ECLAC
Design	Blaine Marcano, ECLAC

Photos: All images in this issue were provided by the winners and finalists of the 'I am a Youth of a Small Island' competition.

Cover: Denisse Aylen González Baez
Within the issue: Katelyn-Elizabeth Hutchinson; Josiah Julipsingh; Cristina Palmer; Evana Marlena Dixon Jackson

Produced by ECLAC

CONTACT INFORMATION

ECLAC Subregional Headquarters for the Caribbean
PO Box 1113, Port of Spain, Trinidad and Tobago
Tel: (868) 224-8000
E-mail: spou-pos@eclac.org Website: www.eclac.org/portofspain

DIRECTOR'S DESK:
WORKING TOWARDS STRONG DATA PROTECTION IN THE CARIBBEAN

Privacy is a fundamental human right, which enables individuals to live with autonomy and dignity and to exercise other rights, like freedom of expression.

Technological innovations, including big data, data profiling and automated decision-making, are exposing the right to privacy to new threats, by reducing the control individuals have over their personal information. Meanwhile, a series of high-profile data breaches affecting millions of people worldwide in recent years has forced into focus the growing range of possible negative consequences that can result from unauthorised access to personal data.

As result of these developments, the issue of data privacy is receiving increased attention across the globe. This has enabled data protection advocates to push for stronger protections for individual privacy rights in a number of countries, including in the Caribbean. The benefits of implementing modern, robust privacy protections go beyond guaranteeing individual rights to facilitating cross-border data flows and trade, creating an enabling environment for e-government and data sharing at the national and regional levels, and creating harmonized data protection standards in the region with potential for cross-border enforcement. The COVID-19 pandemic has highlighted the urgency of delivering better access to e-government services and digital tools across the Caribbean, both to individuals and populations subject to social distancing measures and to bring the pandemic under control by sharing health data and using mobile tools, such as contact tracing apps. Beyond enacting internationally aligned laws, Caribbean countries also have the task of building independent national data protection authorities with the resources to effectively apply and enforce data protection rules.

This issue of FOCUS discusses how Caribbean countries can work together towards strong data protection in the subregion in four areas: aligning data protection legislation with international standards; facilitating data flows between the Caribbean and its trading partners; fostering regulatory cooperation in the subregion in order to harmonise data protection regimes and enable their cross-border enforcement; and creating regulatory and policy tools to provide practical guidance for data users and individuals on their rights and obligations. The range of policy and regulatory tools and their uses are also highlighted, as Caribbean lawmakers and supervisory authorities work towards implementing effective approaches to data protection.

Yours in Focus

Diane Quarless

ECLAC REVIEWS CARIBBEAN DATA PROTECTION LEGISLATION

Amelia Bleeker*

Data protection legislation is being overhauled across the globe, as lawmakers seek to stay one step ahead of the vulnerabilities presented by new data systems. These are responding by creating enhanced protections for personal data and strengthening individual privacy rights. Several Caribbean countries have joined this trend, in drafting and enacting data protection and privacy laws in recent years.

Despite this progress, approximately thirteen countries and territories in the subregion still have no relevant laws in place, while other laws require updating to align with modern data protection principles.

REVIEW OF CARIBBEAN DATA PROTECTION LEGISLATION

ECLAC's recent study, "Creating an enabling environment for e-government and the protection of privacy rights in the Caribbean: A review of data protection legislation for alignment with the General Data Protection Regulation", reviews the data protection laws of six Caribbean countries – Antigua and Barbuda, The Bahamas, Barbados, Belize, Cayman Islands, and Jamaica – for their alignment with the European Union's General Data Protection Regulation (GDPR) and data sharing best practice.[1]

This article outlines the findings of ECLAC's review, highlighting core guarantees and safeguards to include in data protection laws in order to provide a level of protection for personal data which is comparable or 'essentially equivalent' to the GDPR.[2] The GDPR is broadly recognized as international best practice in the area of data protection, and it has extraterritorial scope beyond EU Member States to non-EU data controllers and processors targeting European data subjects.[3] While compliance with the GDPR does not necessarily guarantee compliance with other countries' privacy frameworks, including those in the Caribbean's major trading partner, the US, there is likely to be many shared features and obligations. Therefore, aligning data protection frameworks with the GDPR can offer multiple benefits for Caribbean countries, organizations and individuals beyond facilitating cross-border data flows with EU countries.

FINDINGS OF ECLAC'S REVIEW

In undertaking the review, ECLAC used a series of indicators to assess whether the laws of the six selected countries were fully, substantially, partially or non-aligned with each element of the GDPR.[4]

It is important to note that national data protection laws need not mirror or be fully aligned with each article of the GDPR. Rather, laws should establish the core guarantees and safeguards of the EU regulation as well as the means for ensuring their effective application and enforcement.[5] Therefore, in many cases, substantial or partial alignment with an element of the GDPR can achieve a comparable or an 'essentially equivalent' level of protection for personal data.

Each of the Caribbean data protection laws reviewed in the study has one or more areas of both substantial and partial alignment with the GDPR. Three of the newer laws, Barbados' Data Protection Act 2019, the Cayman Islands' Data Protection Law 2017 and Jamaica's Data Protection Act 2020, have at least one area of full alignment and several areas of substantial alignment. These recently enacted laws have benefited from being drafted to achieve close alignment with international best practice for data protection, following the adoption of the GDPR in 2016. Although the EU regulation came into force in 2018, a draft version was available as early as 2014. As can be observed in Table 1, of the 18 elements in the GDPR, Barbados' DPA 2019 is fully aligned with seven elements and substantially aligned with a further eight. Likewise, Jamaica's 2020 Act has 11 areas of substantial alignment and two areas of full alignment.

* Amelia Bleeker is an Associate Programme Management Officer in the Caribbean Knowledge Management Center of the Economic Commission for Latin America and the Caribbean, Subregional Headquarters for the Caribbean in Port of Spain, Trinidad and Tobago.

[1] A. Bleeker, "Creating an enabling environment for e-government and the protection of privacy rights in the Caribbean: a review of data protection legislation for alignment with the General Data Protection Regulation", Studies and Perspectives series-ECLAC Subregional Headquarters for the Caribbean, No. 94, ECLAC, 2020.

[2] In its *Schrems* I decision, the Court of Justice of the European Union (CJEU) introduced the standard of 'essential equivalence' to assess if the legal regime of a third country provides an adequate level for personal data of European data subjects. See CJEU, *Maximillian Schrems v Data Protection Commissioner*, Case C-362-14, 6 October 2015.

[3] Under the GDPR, 'data subject' is simply defined as an identified or identifiable natural person. 'Personal data' means any information relating to an identified or identifiable natural person.

[4] The indicators used to assess alignment of legislation with the GDPR are included in Annex 1 of ECLAC's study

[5] Guidance on the assessment of the level of data protection in third countries and the core data protection principles that should be present in national data protection systems to achieve essential equivalence with the EU's framework can be found in the 'Adequacy Referential' document of the Article 29 Working Party of EU data protection authorities: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

Table 1: Alignment of selected Caribbean data protection laws with the GDPR

GDPR element	Antigua and Barbuda (2013)	The Bahamas (2003)	Barbados (2019)	Belize (2014)	Cayman Islands (2017)	Jamaica (2020)
Material scope and definitions	Partially aligned	Substantially aligned	Fully aligned	Partially aligned	Substantially aligned	Substantially aligned
Territorial scope	Not aligned	Partially aligned	Fully aligned	Partially aligned	Substantially aligned	Fully aligned
Fundamental principles relating to processing	Substantially aligned	Substantially aligned	Substantially aligned	Substantially aligned	Substantially aligned	Substantially aligned
Lawfulness of processing	Partially aligned	Not aligned	Fully aligned	Partially aligned	Substantially aligned	Fully aligned
Consent	Not aligned	Not aligned	Substantially aligned	Not aligned	Partially aligned	Substantially aligned
Special categories of personal data	Partially aligned	Partially aligned	Substantially aligned	Partially aligned	Substantially aligned	Substantially aligned
Individual rights	Partially aligned	Partially aligned	Fully aligned	Partially aligned	Substantially aligned	Partially aligned
Obligations of data controllers	Partially aligned	Partially aligned	Substantially aligned	Partially aligned	Substantially aligned	Substantially aligned
Obligations of data processors	Partially aligned	Partially aligned	Substantially aligned	Partially aligned	Partially aligned	Partially aligned
Data breach notifications	Not aligned	Not aligned	Fully aligned	Not aligned	Substantially aligned	Substantially aligned
Impact assessments and prior consultation	Not aligned	Not aligned	Fully aligned	Not aligned	Not aligned	Substantially aligned
Data protection officers	Not aligned	Not aligned	Fully aligned	Not aligned	Not aligned	Partially aligned
Codes of conduct and certification	Partially aligned	Partially aligned	Partially aligned	Partially aligned	Partially aligned	Substantially aligned
International transfers	Not aligned	Partially aligned	Substantially aligned	Not aligned	Fully aligned	Substantially aligned
Supervision	Partially aligned	Partially aligned	Substantially aligned	Partially aligned	Substantially aligned	Substantially aligned
Cooperation and mutual assistance	Not aligned	Not aligned	Not aligned	Not aligned	Partially aligned	Partially aligned
Remedies	Partially aligned	Not aligned	Partially aligned	Partially aligned	Partially aligned	Partially aligned
Specific processing situations	Substantially aligned	Not aligned	Substantially aligned	Partially aligned	Substantially aligned	Substantially aligned

Source: Amelia Bleeker, ECLAC

MOST ALIGNED AREAS OF CARIBBEAN DATA PROTECTION LAWS

The material scope and definitions, fundamental principles relating to data processing, conditions to establish lawfulness of processing, and supervisory arrangements were among the elements of the GDPR most reflected in the six laws under review. These features were already well-established in several national data protection laws enacted in the 1990s[6] and the GDPR's predecessor, the 1995 EU Data Protection Directive.[7]

The GDPR introduced new protections to address emerging technologies, given that the 1995 Directive was adopted when the internet was still in its infancy. However, many of the Directive's rules and obligations were carried over into the GDPR, albeit in an enhanced form. Since they reflected best practice before the adoption of the GDPR, some Caribbean countries had adopted them in data protection laws drafted or enacted prior to 2016.

Material scope and definitions

The GDPR applies to the controllers and processors of personal data. A 'data controller' is a person or body that determines the purposes and means of the processing of personal data. A 'data processor' is a person or body who 'processes personal data on behalf of the controller'.

Personal data is defined broadly to include 'any information relating to an identified or identifiable person', or a 'data subject'. Most of the data protection laws considered in the study use the terminology of personal data, data controllers, subjects and processors, with the definitions of these terms being closely or partially aligned to those contained in the GDPR. As noted above, this terminology was already used in EU data protection law prior to the GDPR's adoption, although the GDPR redefined 'personal data' to include new identifiers that could enable the identification of a person, such as location data and online identifiers.

▸ (continued on page 6)

[6] See, for example, the UK's Data Protection Act 1998, which was replaced by the Data Protection Act 2018.
[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

▸ (continued from page 5)

ECLAC REVIEWS CARIBBEAN DATA PROTECTION LEGISLATION *(CONTINUED)*

However, two older Caribbean laws, Belize's Data Protection Bill drafted in 2014 and Antigua and Barbuda's Data Protection Act No. 10 of 2013, define personal data only in relation to 'commercial transactions', which means individuals only gain protection when their personal data is being processed as part of a transaction of a commercial nature. This excludes a wide variety of non-commercial activities carried out by public and private bodies, including for educational, employment, health, taxation, law enforcement, social security and welfare purposes. Furthermore, while most of the laws contain additional, stricter protections for sensitive personal data, the categories of sensitive data included in the GDPR are not always reflected, including personal data relating to sexual orientation and ethnic origin.

Fundamental principles relating to data processing

The GDPR contains seven data protection principles to guide data controllers' use and collection of personal data, which expand on the principles found in the 1995 Directive. A new principle is that personal data must be processed in a manner that ensures security using "appropriate technical or organisational measures". Furthermore, data controllers are now subject to a reinforced principle of accountability requiring them to not only be responsible for but to demonstrate compliance with the data protection principles.

All of the six countries' laws are substantially aligned with these principles, in many cases mirroring the GDPR's language. However, some of them could be enhanced by introducing a GDPR-style accountability principle. This principle pervades the other six data protection principles under the GDPR and aims to encourage a shift towards a proactive approach to the management of personal data.

Lawfulness of processing

Another cornerstone of the GDPR is that personal data can only be processed under one of six conditions, including where consent is given for one or more specific purposes, where it is necessary for the performance of a task carried out in the public interest, and where it is necessary for the legitimate interests of the data controller or a third party. Five out of the six Caribbean countries' laws require data controllers to meet one of a set of conditions in order for the processing of personal data to be lawful. However, there are some differences in the grounds under which processing is lawful, and sometimes the grounds are not elaborated to the same extent as in the GDPR; e.g. consent is required but not for specific purposes.

Supervision

EU Member States are required to establish an independent data protection authority with a board responsible for monitoring the application of the GDPR. All six Caribbean countries' laws establish a data protection supervisory authority but, in some cases, the powers, functions and duties of the authority are not elaborated. Furthermore, not all laws include investigative and corrective powers as extensive as those found in the GDPR.

LEAST ALIGNED AREAS OF CARIBBEAN DATA PROTECTION LAWS

All laws, except Jamaica's Data Protection Act 2020, have at least one area of non-alignment with the GDPR. Several elements of the laws are only partially aligned with the GDPR, creating uncertainty as to whether they would meet the standard of 'essential equivalency' with the EU regulation.

The least reflected areas are provisions relating to consent, cooperation and mutual assistance, international transfers, data breach notifications, data protection impact assessments (DPIAs), prior consultation, and data protection officers. These provisions were only included in a basic form or not at all in some of the Caribbean laws under review, mostly reflecting the state of data protection best practice at the time the laws were drafted. For example, under the 1995 EU Directive, the appointment of data protection officers and the notification of data breaches were not yet mandatory.

Furthermore, countries enacting laws as early as 2003 as in the case of the Bahamas may have overlooked the importance of other elements, such as protections for international transfers and provisions on cooperation and mutual assistance, at a time when global data processing technologies were only in the making and the volume of cross-border data flows was miniscule compared to today. Between 2005 and 2017, cross-border data flows multiplied more than 100 times.[8] Indeed, data protection laws require regularly updating as technological developments, judicial decisions, and implementation and enforcement challenges expose their limitations.

Consent as a lawful ground for data processing

The unambiguous, informed consent of the data subject is a key requirement for data processing under the GDPR. The EU regulation dedicates several articles to clarifying the notion of consent, and defines it as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". While most of the Caribbean laws under review include consent as a ground for data processing, some do not define the term and only require it to be explicit for sensitive personal data. While consent has long been a ground for processing in data

[8] World Bank, 'Trade, Cross-Border Data, and the Next Regulatory Frontier: Law enforcement and data localization requirements', MTI Practice Notes, No. 3, December 2018.

protection laws, the GDPR introduced more stringent requirements for obtaining informed consent.

Cooperation and mutual assistance

Supervisory authorities of EU Member States are required to cooperate and provide mutual assistance to each other, and to develop international cooperation and mutual assistance mechanisms with third countries and international organizations. To facilitate eventual cooperation of this nature, Caribbean data protection laws should also empower local supervisory authorities to engage in cross-border cooperation. Most of the laws reviewed in ECLAC's study are silent on matters of cooperation and mutual assistance, or they make provision for these matters to be dealt with in subsequently drafted regulations. In light of the borderless nature of data flows and processing technologies, making explicit provision for cross-border cooperation and mutual assistance would strengthen the enforcement of Caribbean data protection laws and support the harmonization of legal protections across the subregion.

International transfers of personal data

Personal data may only be transferred outside the EU to countries that provide an adequate level of protection for the rights and freedoms of data subjects. Non-EU countries can apply to the European Commission for an 'adequacy decision' confirming that the country in question offers a level of data protection that is essentially equivalent to that within the EU. Such a decision provides general authority for cross-border transfers. The GDPR also provides for cross-border transfers of personal data subject to 'appropriate safeguards' and limited exceptions. To further align with the GDPR, Caribbean data protection laws should incorporate safeguards for cross-border transfers of personal data to ensure individuals' personal data is not subject to lower standards once transferred to another country. However, international transfers are not dealt with in Belize's Data Protection Bill 2014 or Antigua and Barbuda's Data Protection Act No. 10 of 2013. Furthermore, the Bahamas' Data Protection (Privacy of Personal Information) Act 2003 Chapter 324A does not have adequate safeguards for international transfers or institutional arrangements to facilitate international transfers.

Data breach notifications

One of the GDPR's innovations is a mandatory breach notification requirement, requiring both data controllers and processors to report certain types of personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible. This requirement is an important part of the GDPR's transparency and accountability approach and enables data subjects to exercise legal remedies and mitigate harm caused by serious breaches. Three of the six Caribbean laws under review – those of Antigua and Barbuda, the Bahamas, and Belize – do not contain a requirement to record or report personal data breaches to either data subjects or the supervisory authority. However, the Cayman Islands' Data Protection Law 2017 exceeds the requirements of the GDPR by requiring that data subjects be notified of all breaches, not just where they are likely to result in a high risk to individuals' rights and freedom.

Data protection impact assessments (DPIAs), prior consultation and data protection officers

Prior to the GDPR, EU law did not place direct obligations on data processors. The GDPR has changed this and established several mechanisms by which both data controllers and processors can identify, assess and mitigate risks to personal data. Prior consultation procedures require data controllers to consult with their national supervisory authority in processing situations indicating a high risk to personal data, while DPIAs must be carried out in certain circumstances, such as when using new technologies. Four of the six reviewed Caribbean laws do not incorporate these mechanisms or place direct obligations on data processors.[8] As a result, data controllers and processors have few practical tools for monitoring their use and implementation of appropriate technical and organizational security measures. This in turn limits their ability to take a proactive approach to the management of personal data.

CONCLUSION

Given its reach and impact beyond EU borders, the GDPR is already having global influence and is expected to contribute to the harmonization of data protection laws around the world.[10]

Aligning data protection laws with the EU framework would be advantageous for Caribbean public and private sector organizations who want to facilitate data flows with EU countries and other major trading partners, including the US, and gain competitive advantage in international markets. Implementing internationally aligned legislation can also create an enabling environment for e-government and data sharing in the Caribbean, the urgent need for which has been demonstrated by the COVID-19 pandemic with social distancing measures preventing access to important public services, including education.

To achieve a level of protection comparable to the GDPR, national data protection laws should include modern data protection principles as well as procedural safeguards and enforcement mechanisms to ensure their effective application. New or revised legislation can draw inspiration from approaches taken in other Caribbean jurisdictions, including the recently enacted laws reviewed in ECLAC's study, since several countries in the subregion are putting in place data protection laws incorporating international best practice. ■

[9] Antigua and Barbuda, the Bahamas, Belize and Cayman Islands.

[10] C. Kuner, D. Jerker, B Svantesson, et al, 'The GDPR as a chance to break down borders', International Data Privacy Law 7(4), November 2017, pp. 231–232.

FACILITATING DATA FLOWS AND TRADE BETWEEN THE CARIBBEAN AND ITS TRADING PARTNERS

Amelia Bleeker*

"Personal data is the new oil of the internet and the new currency of the digital world".[1] Global commerce, including between Caribbean countries and their trading partners, relies on the ability of organizations to transfer personal data across borders. In 2014, cross-border data flows contributed an estimated US$2.8 trillion to global GDP.[2] Globalization has moved into a new phase of ever-increasing data flows. Meanwhile, many countries are imposing limitations on the types of data that can be transferred across borders, including data localization rules requiring data to be stored locally.

While personal data should attract privacy protection both within and beyond national borders, limitations on cross-border data flows can carry an economic cost for governments, corporations and individuals alike depending on their nature. The key is therefore to create data protection laws which put in place robust yet enabling frameworks for cross-border data flows.

DATA FLOWS IN AND OUT OF THE CARIBBEAN

In this increasingly connected world, cross-border data flows are the lifeblood of international trade, and they also serve a variety of other critical functions in both the public and private sectors.

For example, e-government functionality requires dynamic pathways of data flow and relies on the ability to transfer personal data securely. The importance of cross-border data flows has been highlighted by the COVID-19 pandemic, with the sharing of health data across the globe and use of cross-border e-health services playing a critical role in the fight against the virus.

Caribbean people benefit from cross-border personal data flows every time they buy an online good or service from another Caribbean country or outside the region. This can be anything from streaming a TV show to using a social media service or buying a book from an online retailer. People outside the subregion benefit from cross-border personal data flows with Caribbean countries when, for example, they book an online service with a Caribbean-based tourism operator or use a financial service provider in the subregion. Furthermore, global businesses operating in the Caribbean, whether in the telecommunications, healthcare, insurance, restaurant and accommodation, aviation, manufacturing, logistics or transportation industries, hold large amounts of personal data of Caribbean nationals and people from around the world.

Caribbean governments also rely on cross-border data flows in several areas, including for national security and crime enforcement purposes and when using remote cloud service providers. Public sector data flows could be increased to improve public service delivery, for example, by using international telemedicine suppliers and software to improve healthcare.

THE ROLE OF DATA PROTECTION LAWS IN FACILITATING CROSS-BORDER DATA FLOWS AND TRADE

Caribbean countries have historically experienced low productivity and performed poorly in the area of international trade. The Caribbean's three largest export markets are the European Union, Latin America and the Caribbean (LAC), and North America, with many untapped markets in Africa, Asia, and other locations.[3]

The subregion is also experiencing a sharp drop in international trade as a result of the economic effects of the COVID-19 pandemic.[4] However, cross-border data flows are transforming international trade and providing new opportunities for Caribbean countries, especially in light of the COVID-19 induced trade slump, to move into new markets and improve productivity by taking advantage of the explosion in digital trade.

Modern data protection legislation has a role to play in achieving this digital transformation by facilitating cross-border data flows, ensuring protection for personal data once it crosses borders, and limiting data localization requirements. Data protection standards build public trust and confidence in online services by protecting individuals' right to privacy. However, data localization, which usually comes in the form of requirements to store data domestically or restrictions on cross-border data flows, acts as a barrier to digital trade.[5] For example, data localisation requirements have hampered the development of mobile money-enabled remittance services, resulting in added costs for migrant workers and their families.[6] Since modern data protection laws often put in place safeguards for the transfer of personal data beyond national borders, they can effectively operate as data localization requirements.

* Amelia Bleeker is an Associate Programme Management Officer in the Caribbean Knowledge Management Center of the Economic Commission for Latin America and the Caribbean, Subregional Headquarters for the Caribbean in Port of Spain, Trinidad and Tobago.

[1] M Kuneva, European Consumer Commissioner, 'Keynote Speech SPEECH/09/156' (Roundtable on Online Data Collection, Targeting and Profiling March 31, 2009)

[2] McKinsey Global Institute, 'Digital Globalization: The New Era of Global Flows', March 2016.

[3] UN COMTRADE via the World Bank's World Integrated Trade Solution (WITS): https://wits.worldbank.org/default.aspx.

[4] UN ECLAC, "The effects of the coronavirus disease (COVID-19) pandemic on international trade and logistics", Special Report, ECLAC, 2020.

[5] Data localization measures exist in the following countries: Australia, Canada (in provinces Nova Scotia and British Columbia), China, Germany, India, Indonesia, Kazakhstan, Nigeria, Russia, South Korea, and Vietnam.

While data protection laws can legitimately seek to ensure that an individual's personal data is not subject to lower standards once transferred to another country, preventing or heavily restricting cross-border data flows does not guarantee data security and may in fact increase its vulnerability. This can be the case for countries in regions prone to extreme weather events like the Caribbean. Caribbean public and private sector organizations are increasingly using remote cloud-based services to prevent data loss following disasters. Rather than heavily restricting cross-border transfers, legislation can put in place enabling safeguards for transfers, such as requiring data sharing and mutual assistance agreements, and facilitate cooperation with other countries on privacy standards and mechanisms for enforcement.

FACILITATING DATA FLOWS WITH THE US AND EU COUNTRIES

Recently enacted Caribbean data protection laws generally follow the European approach of incorporating safeguards for cross-border transfers of personal data. However, international transfers are not dealt with in some laws in the subregion pre-dating the European Union's General Data Protection Regulation (GDPR).[7]

The GDPR permits cross-border transfers of personal data to non-EU countries where the country in question offers a level of data protection that is essentially equivalent to that within the EU. The European Commission issues adequacy decisions certifying that non-EU countries and international organizations offer an adequate level of protection. In lieu of an adequacy decision, data transfers outside the EU are also possible where a third country has in place 'appropriate safeguards'.[8] The most commonly used safeguard is standard contractual clauses (SCCs), whose validity were recently upheld in the Schrems II decision of the Court of Justice of the European Union (CJEU).[9]

In this decision, the CJEU struck down the EU-US Privacy Shield allowing cross-border transfers of data between the US and EU for commercial purposes, on the basis that United States' law does not provide adequate safeguards for the protection of personal data, and European data subjects do not have sufficient actionable rights before US courts. The Court further stated that individually approved SCCs can still be used to transfer personal data from the EU to the US (and other non-EU countries) as long as they provide data subjects with a level of protection essentially equivalent to that guaranteed in EU law. This ruling confirms that, in the absence of an adequacy decision, data controllers in the Caribbean will need to put in place alternative safeguard mechanisms for exporting data to and from the EU, including SCCs and binding corporate rules.

The decision also shed light on the interplay between US and EU data protection standards for Caribbean data controllers transferring personal data to and from these locations. In the absence of a federal-level data protection law, US states have been at the forefront of developing US privacy protections. In particular, the California Consumer Privacy Act (CCPA) 2018 is becoming the de facto standard for companies conducting business in the US, and other states are in the process of drafting similar privacy laws. The CCPA shares some general features with the GDPR, including rights to access and delete personal data and to opt out of data processing.[10] However, the CCPA is focused on consumer privacy rights and disclosures and takes a different approach to consent than the GDPR. In particular, 'opt out' mechanisms are valid under the CCPA, but cannot be used as a means for obtaining consent pursuant to the GDPR.

However, cross-border data transfers are not restricted under the CCPA. Rather, international transfers to 'service providers' require a written agreement containing certain provisions. These differences between the GDPR and the CCPA present potential complications for Caribbean organizations engaging in trade in both locations. While Caribbean data controllers will generally be able to transfer personal data from the US pursuant to a data sharing agreement, SCCs, binding corporate rules or another 'appropriate safeguard' mechanisms found in the GDPR will need to be in place to facilitate cross-border transfers with EU countries.

CONCLUSION

Given the importance of cross-border data flows for e-commerce and international trade, Caribbean countries should endeavour to put in place enabling frameworks for international transfers of personal data.

Depending on the nature of requirements, data protection laws can operate as data localization measures with resulting economic costs. Furthermore, the Schrems II decision has confirmed that, in the absence of an adequacy decision, third country data controllers, including those in the Caribbean, need to put in place 'appropriate safeguards' found in the GDPR to transfer personal data out of Europe. Individually approved SCCs are one commonly used alternative. Transfers of personal data out of the US may be subject to lesser restrictions depending on the laws of the State in question. Nonetheless, data controllers would be well-advised to have in place written data sharing agreements containing certain guarantees for data subjects and addressing questions of liability as a matter of best practice. ■

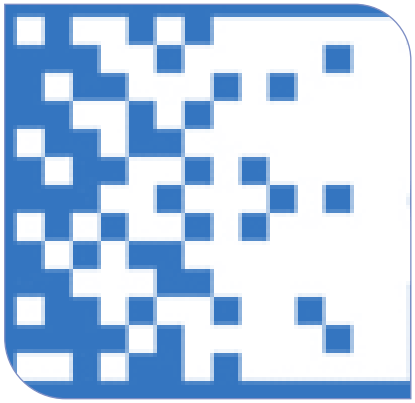
[6] Claire Scharwatt, The impact of data localisation requirements on the growth of mobile money-enabled remittances, GSM Association, 2020.

[7] See, for example, Belize's Data Protection Bill 2014 and Antigua and Barbuda's Data Protection Act (DPA) No. 10 of 2013.

[8] See Article 46(2)-(3) of the GDPR.

[9] SCJEU, Case C-311/18, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, EU:C:2020:559, 16 July 2020.

[10] See the California Consumer Privacy Act (CCPA) 2018 at this link: http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5



REGULATORY COOPERATION IN THE CARIBBEAN AND BEYOND:

THE VALUE OF COLLABORATION ON DATA PROTECTION FROM LEGISLATIVE INCEPTION TO IMPLEMENTATION AND ENFORCEMENT

By the Common Thread Network

Introducing the Common Thread Network (CTN)

The responsible use of personal data and the ability to access official information are rights enjoyed in over 100 countries around the world. Since 2005, more than half of all Commonwealth member countries have either prepared or passed new legislation specifically related to data protection, or amended their existing legislation.

In an increasingly digital world which relies on data flows both within and between jurisdictions, the need to ensure privacy protections for personal data transcends national borders and thus benefits from global cooperation by regulators. Similarly, the privacy challenges created by technological innovations are the same in the Caribbean as they are in Europe, Africa, Asia, the Pacific, and the Americas. Regulators need to anticipate new data systems and technological innovations, and pre-empt the inevitable challenges in the interplay between theoretical standards (the legislation) and practical implementation. Collaboration on these systemic societal issues allows better regulation for our data subjects.

One means of collaboration is through the Common Thread Network (CTN), a concept which originated in the margins of the 2013 International Conference of Data Protection and Privacy Commissioners (now the Global Privacy Assembly) when the data protection and privacy enforcement authorities of the Commonwealth countries agreed in principle to establish a network to facilitate more regular and formal contact. Although recognizing the inherent diversity of the Commonwealth, there is a shared background in language, culture and the rule of law; and unity through shared values and principles (Commonwealth Charter). The work of the Common Thread Network is essentially driven by its participants and revolves around two general themes: 1) promoting good privacy practices to assist socio-economic development; and 2) acting as a platform to promote cross-border cooperation and build capacity by sharing knowledge on emerging trends, regulatory changes and best practices for effective data protection.

As an example, representatives from the jurisdiction of Bermuda have enjoyed the benefits of various types of involvement with the Common Thread Network, from the early days of drafting privacy laws to full membership. Prior to the creation of the country's regulatory office, representatives from Bermuda's government attended CTN meetings as Observers to discuss the merits and lessons learned from a variety of regulatory regimes and legal language.

Commissioner Alexander White of the Office of the Privacy Commissioner for Bermuda, which became a full member of CTN in May 2020, describes how the ready access to colleagues and counterparts accelerated his work. In addition to an ability to meet with and receive advice from experienced regulators in similar jurisdictions, CTN Members assisted with both strategic advice and logistical matters such as template job descriptions, policies and procedures, and even public awareness materials. "I am very grateful for the opportunity to sit down with colleagues (or, video chat as we all do now) to discuss ideas or approaches, and what worked for them. It allowed the Office to bypass some early growing pains, and has certainly been a benefit in the quickly-changing COVID-19 response."

A similar sentiment is shared by Deputy Ombudsman for Information Rights, Jan Liebaers, of the Office of the Ombudsman Cayman Islands. He explains that ongoing commitments are needed when new legislation is introduced to ensure its objectives are met. The drafting and passing of legislation is the first step, but enacting it requires the establishment and funding of a data protection authority, outreach, guidance materials, training etc. and, subsequently, the processes and means to enforce standards and obligations when they are not upheld. To ensure successful implementation, CTN supports the recommendation made in ECLAC's recent study, "Creating an enabling environment for e-government and the protection of privacy rights in the Caribbean: A review of data protection legislation for alignment with the General Data Protection Regulation", that countries adopt data protection instruments that enable effective domestic and cross-border enforcement, and which make provision for cooperation between supervisory authorities.

COMMUNITY OF PRACTICE IN SUPPORT OF IMPLEMENTING AND REGULATING DATA PROTECTION AND PRIVACY FRAMEWORKS

The global pandemic has underscored the dual role that data protection plays in response to novel societal challenges: good data protection is an enabler of innovation, but it must also protect and respect the rights of people whose data – and trust – such projects rely on.

Indeed, the COVID-19 pandemic has accelerated the pace of digitalization, and this, in turn, has strengthened the requirement for 'privacy by design' to be front and foremost in proposed responses, and to guard against so-called

'mission creep'.

Over the last six months, engagement with global counterparts has helped to inform our respective regulatory responses to issues as varied as COVID-19 exposure notification apps; the efficacy of temperature testing in airports and public places; questions of 'proportionate' and 'necessary' data sharing and how these terms can and should be construed in the context of a global pandemic; as well as the ongoing challenges of regulating emerging technology or cross-border data flows. Such engagement allows regulators to sense-check their positions, leverage best practice from countries that are more experienced in a particular field, as well as share experience and expertise to provide for greater confidence and consistency in approaches to the protection of personal data. This is true too of the need for codes of practice or detailed guidance to support businesses with the practical application of provisions, where there may be efficiencies in sharing products.

Within the Network, community participants are varied, reflecting that some of the countries or territories they represent have dedicated data protection laws, while others have legislation under development. The invitation to Commonwealth governments that do not yet have data protection legislation and/or a corresponding regulator to join the Common Thread Network (as an Observer) is novel among global and regional data protection and privacy fora. This openness to both established and nascent data protection cultures underscores the essence of the modern-day Commonwealth as an association of equal countries, thus affirming a role for CTN in advocating for the differing needs of Member States, from policy advice to delivering technical assistance.

BUILDING ON SHARED PRINCIPLES PRIVACY FRAMEWORKS

In bringing together Commonwealth countries, the Common Thread Network is a global endeavour, with representation from Europe, Africa, Asia, the Pacific, the Americas and the Caribbean (the Bahamas, Bermuda, the Cayman Islands, and Trinidad and Tobago).

There are currently 18 Member authorities (and a further four Observers), and 22 fully enacted pieces of data protection legislation. These instruments differ in their scope (e.g. as applicable to private versus public sector; state or federal) and in the supervisory reach of the Data Protection Authority (e.g. advisory, investigative, corrective) but they nevertheless share principles to which all members subscribe. It is acknowledged that there will always be differences in cultural, contextual and legal constructs between jurisdictions, and the global privacy community, of which CTN is a part, seeks to navigate these differences and encourage interoperability and alignment with relevant international standards.

In April 2018, the Commonwealth Heads of Government adopted the Declaration on the Commonwealth Connectivity Agenda for Trade and Investment and the Commonwealth Cyber Declaration. Both declarations recognize the importance of regulatory frameworks and together set out a Commonwealth approach to digital economies and intra-Commonwealth trade, investment and development. The Connectivity Agenda highlights the importance of understanding regulatory regimes, increasing the ease of doing business and promoting good regulatory practice. The Commonwealth Cyber Declaration emphasizes the importance of common standards and the strengthening of data protection and security frameworks, in order to promote public trust in the internet, confidence for trade and commerce, and the free flow of data.

CTN comprises countries representing all stages of the evolution of data protection and privacy regimes: from countries yet to introduce privacy legislation, to countries with nascent data protection regimes that are educating controllers or undertaking enforcement activity for the very first time, through to countries with mature frameworks and established supervisory authorities that are working to modernise their instruments to make them fit for the 21st century. For example, New Zealand's updated Privacy Act will come into force on 1 December 2020 (replacing the 1993 Act); and the Canadian federal government has now commenced review of both the federal public and private sector privacy statutes (responding to collective calls from the federal, provincial and territorial information and privacy commissioners for privacy law reform in both private and public sectors).

In short, whatever the maturity of a data protection framework, there is a need to regularly review and scrutinize the context for which it is – or was – intended, and to subscribe to the ethos of continuous improvement – from an economic, societal and rights-based perspective. In this endeavour, sharing the challenges of legislative gaps or deficiencies, or barriers to implementation or enforcement, can enrich the work of all regulators.

Furthermore, as Bermuda's Commissioner White points out: "Like many of the countries in the Greater Caribbean, due to our size we depend on cross-border data transfers to leverage vendors based overseas. By collaborating we give our region an opportunity to be more influential on both data protection policy and the practices of larger organizations."

To find out more about the Common Thread Network and to apply to join us, see https://www.commonthreadnetwork.org/ or contact the Secretariat at CTN-Secretariat@ico.org.uk. ■

DEMYSTIFYING DATA PROTECTION LAWS THROUGH REGULATORY AND POLICY TOOLS TO GUIDE THE APPLICATION OF LEGISLATION

Amelia Bleeker*

In recent years, lawmakers around the world have enacted a raft of data protection laws promising to give individuals greater control over their personal data. These pieces of legislation are often long and complex, which can make privacy rights and obligations difficult to understand. As a result, policy makers have worked in concert with legislators to provide practical guidance - via regulatory and policy instruments - on the requirements of new laws.

Since an effective approach to data protection must overcome institutional and cultural and legal barriers, these instruments can form part of a comprehensive approach to encourage compliance with new privacy guarantees. Policy guidance can be particularly useful for small and medium-size organizations that lack the legal resources to translate their data processing obligations into layperson terms. Such guidance can be created by lawmakers, industry or technical bodies, data protection authorities or data protection officers appointed to oversee data processing activities of certain organizations. This article provides information on the choice of regulatory and policy instruments available to supervisory authorities and other parties tasked with implementing new data protection frameworks.

EXAMPLES OF REGULATORY AND POLICY TOOLS FOR DATA PROTECTION AT THE NATIONAL LEVEL

Data protection legislation often provides for the making of regulations and the drawing up of guidelines and/or codes of practice or conduct – either by the national data protection authority or bodies representing data controllers – in order to guide the application of data protection principles.

These tools can be aimed generally at data controllers and processors or data subjects or, alternatively, provide specific guidance for certain sectors or complex data protection issues.

Jamaica's Data Protection Act 2020 - enacted this year - demonstrates the range of regulatory and policy tools that can be built into legislation to guide the application of data protection principles. Under the Act, the Information Commissioner must prepare a data-sharing code (section 57) as well as a code of practice for assessment notices (section 47). Regulations may be made for the purpose of giving effect to the provisions of the Act, including in several specific areas set out in section 74. The Act also makes provision for the Commissioner preparing, or directing the preparation of, guidelines as to good practice (section 4(5)(e)) and for trade associations to prepare self-initiated guidelines (section 4(5)(f)).

In Europe, the supervisory authorities of EU Member States are required to encourage the drawing up of codes of conduct by associations and other bodies representing categories of controllers or processors, and to approve and monitor such codes (GDPR, Arts. 40-41). Ideally, codes of conduct should be accompanied by a certification mechanism for monitoring data controllers' compliance with the code (GDPR, Art. 42). The United Kingdom's Data Protection Act 2018 requires the Information Commissioner to prepare a data sharing code of practice containing practical guidance in relation to the sharing of personal data in accordance with the requirements of the legislation and good practice (section 121).

Table 2 gives some further examples of regulatory and policy instruments supplementing data protection legislation in several Caribbean countries and from a selection of other English-speaking jurisdictions with data protection regimes.

TYPES OF POLICY AND REGULATORY TOOLS AVAILABLE

As highlighted in Table 2, the main policy and regulatory tools available to provide guidance on the requirements of data protection legislation include:

- Regulations providing details on the operation of legislative provisions,
- Ministerial orders to modify the application of the legislation in certain areas;
- Codes of conduct and practice;
- Guidelines containing data protection best practice; and
- Self-initiated codes of conduct for certain sectors or industries.

The range of tools available to policymakers is usually circumscribed by the legislation in question e.g. where regulations in certain areas are mandated, but there is usually some flexibility to prepare tools for certain sectors or data protection issues as warranted by the national context and the needs of certain categories of data controllers and processors.

* Amelia Bleeker is an Associate Programme Management Officer in the Caribbean Knowledge Management Center of the Economic Commission for Latin America and the Caribbean, Subregional Headquarters for the Caribbean in Port of Spain, Trinidad and Tobago.

Table 2: Examples of regulatory and policy instruments supplementing data protection legislation in selected countries

Caribbean countries and territories	*Legislation*	*Regulatory and policy instruments provided for in legislation*	*Adopted regulatory and policy instruments*
The Bahamas	Data Protection (Privacy of Personal Information) Act 2003 Chapter 324A	Codes of practice for categories of data controllers (section 20) Regulations (section 30)	Guide for Data Controllers
Cayman Islands	Data Protection Law (DPL) 2017	Codes of practice (section 42) Regulations (section 61)	Data Protection Regulations 2018 Guide for Data Controllers: Data Protection Law 2017 Guidance on Monetary Penalties
Jamaica	Data Protection Act (DPA) 2020	Regulations (section 74) Data-sharing code (section 57) Code of practice for assessment notices (section 47) Guidelines as to good practice (section 4(5)(e)) Self-initiated guidelines for trade associations (section 4(5)(f))	N/A – legislation recently enacted
Other countries	*Legislation*	*Regulatory and policy instruments provided for in legislation*	*Adopted regulatory and policy instruments*
Australia	Privacy Act 1998	Privacy codes (Part IIIB) Regulations (section 100) Guidelines in a number of areas (sections 26V, 28 and 95)	Australian Privacy Principles guidelines Best Practice Guide to Applying Data Sharing Principles
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA) Privacy Act, R.S.C. 1985, c P-21	Organizational codes of practice (section 24) Model Code for the Protection of Personal Information of the Canadian Standards Association (schedule 1) Guidelines (section 23) Procedures for sharing information (section 23) Regulations (sections 26 and 48)	Privacy Guide for Businesses CSA Model Code for the Protection of Personal Information (CAN/CSA-Q830-96; published March 1996; reaffirmed 2001)
New Zealand	Privacy Act 1993 Privacy Act 2020 (Note: The Privacy Act 2020 will replace the 1993 Act on 1 December 2020 and bring in new codes of practice)	Information Privacy Principles (Privacy Act 2020, sections 22-31) Codes of practice (Privacy Act 2020, sections 32-38) Regulations (Privacy Act 2020, sections 213-215)	New codes of practice to be created under Privacy Act 2020. Codes published under 1993 Act: Health Information Privacy Code 1994 Civil Defence National Emergencies (Information Sharing) Code 2013 Credit Reporting Privacy Code 2004 Justice Sector Unique Identifier Code 1998 Superannuation Schemes Unique Identifier Code 1995 Telecommunications Information Privacy Code 2003
United Kingdom	Data Protection Act 2018	Codes of practice, including data sharing, direct marketing and journalism codes (sections 121-128) Regulations (sections 16, 137, 182) Guidance about fees (section 136) Guidance about privileged communications (section 133)	Guide to Data Protection Data Sharing Code of Practice (currently being updated) Guide to Privacy and Electronic Communications

Source: Amelia Bleeker, ECLAC

Supervisory authorities can also create other non-binding tools, such as toolkits and audit checklists for data controllers and processors and awareness-raising materials for data subjects, pursuant to their duty to inform the public and promote awareness about data protection rights and obligations.[1] Such tools assist data controllers to proactively identify and minimize risks to personal data and implement appropriate security measures. Where legislation requires certain public and private organizations to appoint data protection officers,[2] the designated officer can also create policy tools in order to encourage the organization's compliance with the law.

Regulations and ministerial orders

As a form of secondary legislation, regulations contain legally binding rules that flesh out details regarding the operation of primary legislation. The Cayman Islands' Data Protection Regulations 2018 supplement the Data Protection Law 2017 by providing additional details and rules in relation to personal data requests, duties of data controllers, and certain exemptions under the Law. Ministerial orders are a form of tertiary legislation found in some Caribbean data protection laws, usually enabling Ministers to make exceptions to or modify the application of individual rights and other protections.

As a basic principle, primary legislation should establish core data protection standards, rights and obligations. This can prove especially important when there is a period between primary legislation coming into effect and the making of regulations. For example, while regulations can be used to flesh out the modalities of mutual assistance and cooperation with other supervisory authorities, primary legislation should include an obligation to cooperate and provide mutual assistance in cases of cross-border personal data transfers.

▸ (continued on page 14)

[1] See, for example, the functions of Barbados' Data Protection Commissioner in section 71 of the Data Protection Act 2019.
[2] See sections 67-69 of Barbados' Data Protection Act 2019 as an example.

▸ (continued from page 13)

DEMYSTIFYING DATA PROTECTION LAWS THROUGH REGULATORY AND POLICY TOOLS TO GUIDE THE APPLICATION OF LEGISLATION *(CONTINUED)*

Data protection legislation should also include safeguards to ensure that regulations and ministerial orders are subject to independent oversight in the form of parliamentary or judicial scrutiny. Such oversight can help to ensure the necessity and proportionality of the proposed secondary or tertiary legislation. In the Caribbean, some pieces of data protection legislation permit ministerial orders to be made limiting the application of data protection rights without judicial or parliamentary scrutiny.[3] Independent oversight offers an important check on executive power and should be built into any delegated law-making powers in order to ensure respect for the rule of law.

Guides, codes of conduct and other non-binding tools

Policy guidance can be general in nature, such as the 'Guides for Data Controllers' used in the Bahamas and the Cayman Islands to guide the interpretation of those countries' legislation. As the name 'guide' suggests, these documents offer non-binding guidance to data controllers processing personal data in those jurisdictions. There are no direct consequences for failing to comply with such guidance, unless the failure is also a breach of the legislation in question. However, since compliance with a 'guide' or other non-binding guidance can offer the best indication of how to adhere to primary legislation, data controllers will usually treat them as offering more than mere advice. Furthermore, while the name of an instrument is usually a good indicator of whether it is legally binding or non-binding, documents with similar names can have different legal effects. For example, in some countries, privacy codes contain legally binding rules e.g. New Zealand's Health Information Privacy Code 1994, while, in others, they offer mere guidance e.g. the United Kingdom's Data Sharing Code of Practice.

Sector or issue-specific codes of conduct can also be used to provide more detailed guidance on complex privacy issues or to give special protection to categories of sensitive personal data. As an example of the latter, New Zealand created a Health Information Privacy Code 1994 to give extra protection to health information because of its sensitivity. The country also has five other privacy codes, including one for telecommunications information.[4] Where the subject matter of a proposed code is technical, legislation usually recognizes that an industry regulator or technical body is best suited to prepare and disseminate this guidance following the approval of the country's data protection supervisory authority.

A note on data sharing codes

Modern data protection legislation is increasingly requiring the creation of data sharing codes in order to incentivize and provide clear guidance on lawful data sharing. Given that the sharing of data can run counter to modern data protection principles and its importance for economic growth, policymaking and innovation, special guidance in this area should be encouraged. For example, Jamaica's Data Protection Act 2020 requires the creation of a data-sharing code containing practical guidance on the sharing of personal data in accordance with good practice and the requirements of the Act. The creation of data sharing codes in the Caribbean would be a positive development, since increased inter-regional data sharing could address data shortages, facilitate data and trade flows between countries, and contribute to region-wide solutions for common issues.

CONCLUSION

To make privacy rights accessible to the public and ensure data controllers and processors understand their obligations, lawmakers should strive to make data protection legislation as concise and easy to understand as possible.

Policy and regulatory tools should not be used in place of clear, user-friendly legislation. However, where substantive provisions of data protection laws require detailed machinery to bring them into operation, regulations are the most used tool to flesh out those details. Data protection legislation can also provide for a selection of policy tools as appropriate for the national privacy landscape in order to overcome institutional and other barriers to effective data protection. Beyond legislators and supervisory authorities, data protection officers can also create policy guidance and tools for the public and private sector organizations whose data processing activities they are tasked with overseeing. ■

[3] See ECLAC's study "Creating an enabling environment for e-government and the protection of privacy rights in the Caribbean: a review of data protection legislation for alignment with the General Data Protection Regulation" for further discussion of this topic

[4] Telecommunications Information Privacy Code 2003 (New Zealand). These codes are soon to be replaced by new codes under New Zealand's new Privacy Act 2020, which replaces and repeals the Privacy Act 1993.

RECENT AND UPCOMING MEETINGS

2020

MARCH

31 March 2020
The Escazú Agreement: towards the implementation of the 2030 Sustainable Development Agenda (Seminar for public officials)

APRIL

1 April 2020
The Escazú Agreement: towards the implementation of the 2030 Sustainable Development Agenda (Seminar for Civil Society Representatives and interested stakeholders)

List of Recent ECLAC Documents and Publications

Listed by Symbol Number, Date and Title

LC/CAR/TS.2019/8 January 2020
Industrial upgrading and diversification to address competitiveness challenges in the Caribbean: The case of tourism

LC/CAR/TS.2019/9 January 2020
A review of Caribbean national statistical legislation in relation to the United Nations Fundamental Principles of Official Statistics

LC/CAR/TS.2019/7 January 2020
The enhancement of resilience to disasters and climate change in the Caribbean through the modernization of the energy sector

LC/CAR/TS.2019/12 January 2020
Promoting debt sustainability to facilitate financing sustainable development in selected Caribbean countries: A scenario analysis of the ECLAC debt for climate adaptation swap initiative

The Magazine of the Caribbean Development and Cooperation Committee
ECLAC Subregional Headquarters for the Caribbean

PO Box 1113, Port of Spain, Trinidad and Tobago
Tel: 868-224-8000
E-mail: eclac-spou-pos@eclac.org

vrb.al/eclaccaribbean